

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-334511

(43)Date of publication of application : 22.11.2002

---

(51)Int.Cl. G11B 20/10  
G06F 3/06  
G06F 12/14  
G11B 7/004  
G11B 27/00

---

---

(21)Application number : 2002-022360 (71)Applicant : SONY COMPUTER ENTERTAINMENT INC  
(22)Date of filing : 30.01.2002 (72)Inventor : KUTARAGI TAKESHI  
OKAMOTO SHINICHI  
MIURA KAZUO

---

(30)Priority

Priority number : 2001022811 Priority date : 31.01.2001 Priority country : JP

---

### (54) COMPUTER SYSTEM AND ITS USING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a computer system having an authentication system which verifies whether an optical disk is illegally used or not.

SOLUTION: In the computer system many computers to which optical disks can be loaded can be connected to an authenticating server through a network and each computer has a peculiar device ID and the server has a user database where the device ID is stored at the time of using the computer and a disk ID is stored at the time of using an optical disk and data of a pair of the disk ID and the device ID is stored in the user database. When the optical disk is used at the second and following times disk ID data and device ID data are transmitted to the authenticating server from the computer through the network to authenticate the normal use.

---

### CLAIMS

---

[Claim(s)]

[Claim 1] In a network system provided with the 1st information processor with which it is equipped with the 1st recording medium and the 1st information processor and the 2nd information processor connected via a network Peculiar information relevant to the 1st information processor in the 2nd information processor A network system which receives peculiar information relevant to the 1st recording medium from said 1st information processor is connected or contained in the 2nd information processor and attests a recording medium by referring to information in a database in which accumulation, elimination, etc. of information are possible and each received peculiar information.

[Claim 2] A network system to which this network system accumulates peculiar information relevant to the 1st information processor or 1st recording medium into a database with the 2nd information processor further in the network system according to claim 1.

[Claim 3] A network system to which the network system according to claim 1 accumulates peculiar information relevant to the 1st information processor and 1st recording medium into a database with the 2nd information processor further.

[Claim 4] A network system which is the peculiar information relevant to said 1st information processor or the 1st recording medium with which information in a database was beforehand recorded in the network system according to any one of claims 1 to 3.

[Claim 5] A network system which is the peculiar information relevant to said 1st information processor and the 1st recording medium with which information in a database was beforehand recorded in the network system according to any one of claims 1 to 3.

[Claim 6] A network system with which information in a database is updated in the network system according to claim 2 or 3 by newly accumulated information.

[Claim 7] A network system which accumulates peculiar information relevant to the 1st information processor or 1st recording medium into a database in the network system according to any one of claims 2 to 6 when a recording medium is used unjustly.

[Claim 8] A network system with which the network system according to any one of claims 1 to 7 makes possible or impossible further processing performed in the 1st information processor by the 2nd information processor.

[Claim 9] A network system with which the network system according to any one of claims 1 to 8 makes possible or impossible reading processing of a program further recorded on the 1st recording medium performed in the 1st information processor by the 2nd information processor.

[Claim 10] An enabling signal with which the 2nd information processor enables processing which should be performed by the 1st information processor in the network system according to claim 8 or 9 Or a network system which transmits a refusal signal which makes impossible processing which should be performed by the 1st information processor.

[Claim 11] A network system which enables processing performed by the 1st

information processor when information applicable to peculiar information relevant to the 1st recording medium is accumulated into a database in the network system according to claim 10 as a result of reference by the 2nd information processor.

[Claim 12]In the network system according to claim 10it is accumulated into a database as information with which peculiar information relevant to the 1st information processor and peculiar information relevant to the 1st recording medium were relatedPeculiar information relevant to said 1st information processor that the 2nd information processor receivedand peculiar information relevant to the 1st recording medium as a result of reference by the 2nd information processorA network system which enables processing performed by the 1st information processor device when in agreement with associated information in a database.

[Claim 13]In the network system according to claim 9a program is enciphered and recorded on the 1st recording mediumand the 2nd information processorthe 1st -- an information processor -- a network system which makes possible reading processing of the 1st recording medium by the 1st information processor by transmitting information for decoding a program in the 1st enciphered recording medium.

[Claim 14]A network system whose information for decoding in the network system according to claim 13 is a key for decryption.

[Claim 15]The network system according to any one of claims 1 to 14It is connected to the 3rd information processor with which it is equipped with the 2nd recording medium different furthermore from the 1st recording mediumand the 2nd information processor receives peculiar information relevant to the 1st recording medium from the 1st information processorand. A network system which receives peculiar information relevant to the 2nd recording medium from the 3rd information processor.

[Claim 16]The network system according to claim 15Peculiar information relevant to the 1st recording medium received from the 1st information processor with the 2nd information processorit was referred to with reference to peculiar information relevant to the 2nd recording medium received from the 3rd information processor -- eachwhen peculiar information overlapsA network system which makes possible or impossible reading processing of a program recorded on the 2nd recording medium performed in the 3rd information processor.

[Claim 17]A network system which the network system according to claim 16 makes possible further executive operation of the 2nd recording medium with which the 2nd information processor is performed in the 3rd information processor to the 1st information processoror transmits confirmed information about no.

[Claim 18]A network system which makes executive operation of the 2nd recording medium possible in the 3rd information processor when consent has the 2nd information processor from the 1st information processor in the network system according to claim 17.

[Claim 19]In the network system according to any one of claims 1 to 18to the 1st information processorwearing of the 3rd recording medium is still enabled and the

2nd information processorAfter receiving peculiar information relevant to the 1st information processor received from the 1st information processorand peculiar information relevant to the 1st recording mediumeach -- transmitting peculiar information to the 1st information processor -- the 1st information processor -- each -- a network system which accumulates peculiar information into the 2nd recording medium.

[Claim 20]A network system which refers to peculiar information relevant to the 1st recording medium in the 1st information processorand information accumulated into the 3rd recording medium in the network system according to claim 19.

[Claim 21]A result of reference according [ on the network system according to claim 20 and ] to the 1st information processorA network system which enables processing performed by the 1st information processor when information applicable to peculiar information relevant to the 1st recording medium is accumulated into the 3rd recording medium.

[Claim 22]A network system whose peculiar information on said network system according to any one of claims 1 to 21 and relevant to an information processor is apparatus ID.

[Claim 23]A network system whose peculiar information on said network system according to any one of claims 1 to 22 and relevant to an information processor is user ID.

[Claim 24]A network system whose peculiar information on said network system according to any one of claims 1 to 22 and relevant to said recording medium is recording-medium ID.

[Claim 25]A computer system whose recording medium which recorded said application is an optical disc in the computer system according to claim 1 and in which said recording-medium ID is disk ID.

[Claim 26]A computer system by which said disk ID is recorded on a field in a data area of said optical discor fields other than a data area in the computer system according to claim 25.

[Claim 27]A computer system from which said disk ID is detected by said computer in the computer system according to claim 25 based on an address of disk ID information recorded on a data area of said optical disc.

[Claim 28]A computer system by which said disk ID is recorded on a disk with organic coloring matter in the computer system according to claim 25.

[Claim 29]A computer system currently formed in the computer system according to claim 25 by a method by which said disk ID used a physical change of a pit sequence.

[Claim 30]A computer system for which a method using a physical change of said pit sequence uses either change of a radial direction of a pit sequencechange of the direction of a minor axis of pit size or change of a depth direction of a pit in the computer system according to claim 29.

[Claim 31]A computer system currently formed in the computer system according to claim 25 by a method by which said disk ID used digital watermarking.

[Claim 32]In a method of attesting this recording medium using the 1st information processor with which it is equipped with the 1st recording mediumand a network system which has the 1st information processor and the 2nd information processor connected via a networkA step which receives peculiar information relevant to the 1st information processor from said 1st information processor in the 2nd information processorand peculiar information relevant to the 1st recording mediumA method which the 2nd information processor is connected or contained in the 2nd information processorand contains a step which attests the 1st recording medium by referring to information in a database in which accumulationeliminationetc. of information are possibleand each received peculiar information.

[Claim 33]Are the 1st information processor with which it is equipped with the 1st recording mediumand in the 2nd information processor and the 1st information processor connected via a network this 1st information processorInformation in a database which transmits peculiar information relevant to the 1st information processorand peculiar information relevant to the 1st recording medium to said 2nd information processorand is connected or contained in the 2nd information processor and in which accumulationeliminationetc. of information are possibleThe 1st information processor that attests the 1st recording medium by referring to each transmitted peculiar information.

[Claim 34]In the 1st information processor with which it is equipped with the 1st recording mediumand the 2nd information processor connected via a networkthis 2nd information processorInformation in a database which receives peculiar information relevant to the 1st information processorand peculiar information relevant to the 1st recording medium from said 1st information processorand is connected or contained in the 2nd information processor and in which accumulationeliminationetc. of information are possibleThe 2nd information processor that attests the 1st recording medium by referring to each received peculiar information.

[Claim 35]In a recording medium which is performed with the 2nd information processor connected via the 1st information processor and a network with which it is equipped with the 1st recording medium and which recorded a program which can be executed [ that reading is possible and ] with this 2nd information processorA step which receives peculiar information relevant to the 1st information processor in this programand peculiar information relevant to the 1st recording medium from said 1st information processorA recording medium which is connected or contained in the 2nd information processorand contains a step which attests the 1st recording medium by referring to information in a database in which accumulationeliminationetc. of information are possibleand each received peculiar information.

[Claim 36]. Are the 1st information processor with which it is equipped with the 1st recording mediumand perform with the 2nd information processor and the 1st information processor connected via a network. In a recorded recording mediuma program which can be executed [ that reading is possible and ] with this 1st

information processor this programA step which transmits peculiar information relevant to the 1st information processorand peculiar information relevant to the 1st recording medium to said 2nd information processorA recording medium which is connected or contained in the 2nd information processorand contains a step which attests the 1st recording medium by referring to information in a database in which accumulationeliminationetc. of information are possibleand each transmitted peculiar information.

[Claim 37]In a program which can be executed [ that reading is possible and ] with this 2nd information processor performed with the 1st information processor with which it is equipped with the 1st recording mediumand the 2nd information processor connected via a networkA step which receives peculiar information relevant to the 1st information processorand peculiar information relevant to the 1st recording medium from said 1st information processorA program which is connected or included in the 2nd information processorand contains a step which attests the 1st recording medium by referring to information in a database in which accumulationeliminationetc. of information are possibleand each received peculiar information.

[Claim 38]. Are the 1st information processor with which it is equipped with the 1st recording mediumand perform with the 2nd information processor and the 1st information processor connected via a network. In a program which can be executed [ that reading is possible and ] with this 1st information processorA step which transmits peculiar information relevant to the 1st information processorand peculiar information relevant to the 1st recording medium to said 2nd information processorA program which is connected or included in the 2nd information processorand contains a step which attests the 1st recording medium by referring to information in a database in which accumulationeliminationetc. of information are possibleand each transmitted peculiar information.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the authentication system which verifies whether recording mediasuch as an optical discare used improperly.

[0002]

[Description of the Prior Art]Various kinds of programs can be executed in the computer which equips with and uses an optical disc. One of such the computers has an entertainment systemand it is typically used as a game device. In such an entertainment systemthe optical disc in which the game program was recorded is purchasedand a game is performed. An entertainment system is connected with the contents server which accumulated many game programs via a networkand what downloads and purchases a game program via a network is planned these days.

[0003]

[Problem(s) to be Solved by the Invention]The optical disc which recorded the purchased optical disc or the downloaded program may be used unjustly. That is the optical disc which recorded the program does not have permission of the owner of a copyright about a program and may be copied unjustly or may be sold considering this as a used article. if such a state is neglected the owner of a copyright cannot collect just profits -- the volition of program creation -- \*\* -- \*\*\*\* -- it becomes things.

[0004]

[Means for Solving the Problem]In view of an above-mentioned problem an object of this invention is to provide a computer system which has an authentication system which verifies whether recording media such as an optical disc are used improperly.

[0005]An object of this invention is to provide the directions for a computer system which has an authentication system which verifies whether recording media such as an optical disc are used improperly.

[0006]The 1st information processor (for example entertainment device of 1) with which has for a network system concerning this invention it is equipped with the 1st recording medium (for example optical disc) Are the 1st information processor and the 2nd information processor (for example server for attestation) connected via a network the network system which it had and the 2nd information processor Peculiar information (for example apparatus ID) relevant to the 1st information processor Peculiar information relevant to the 1st recording medium is received from said 1st information processor it is connected or contained in the 2nd information processor and a recording medium is attested by referring to information in a database in which accumulation elimination etc. of information are possible and each received peculiar information.

[0007]A network system concerning this invention is an above-mentioned network system and this network system accumulates peculiar information relevant to the 1st information processor or 1st recording medium into a database with the 2nd information processor further.

[0008]A network system concerning this invention is an above-mentioned network system and accumulates peculiar information relevant to the 1st information processor and 1st recording medium into a database with the 2nd information processor further.

[0009]A network system concerning this invention is an above-mentioned network system and information in a database is peculiar information relevant to said 1st information processor or the 1st recording medium recorded beforehand.

[0010]A network system concerning this invention is an above-mentioned network system and information in a database is peculiar information relevant to said 1st information processor and the 1st recording medium which were recorded beforehand.

[0011]A network system concerning this invention is an above-mentioned network system and information in a database is updated by newly accumulated information.

[0012]A network system concerning this invention is an above-mentioned network system and when a recording medium is used unjustly it accumulates peculiar information relevant to the 1st information processor or 1st recording medium into a database.

[0013]A network system concerning this invention is an above-mentioned network system and makes possible or impossible further processing performed in the 1st information processor by the 2nd information processor.

[0014]A network system concerning this invention is an above-mentioned network system and makes possible or impossible reading processing of a program further recorded on the 1st recording medium performed in the 1st information processor by the 2nd information processor.

[0015]A network system concerning this invention It is an above-mentioned network system and the 2nd information processor transmits an enabling signal which enables processing which should be performed by the 1st information processor or a refusal signal which makes impossible processing which should be performed by the 1st information processor.

[0016]A network system concerning this invention It is an above-mentioned network system and when information applicable to peculiar information relevant to the 1st recording medium is accumulated into a database as a result of reference by the 2nd information processor processing performed by the 1st information processor is enabled.

[0017]A network system concerning this invention Are an above-mentioned network system and it is accumulated into a database as information with which peculiar information relevant to the 1st information processor and peculiar information relevant to the 1st recording medium were related Peculiar information relevant to said 1st information processor that the 2nd information processor received and peculiar information relevant to the 1st recording medium as a result of reference by the 2nd information processor When in agreement with associated information in a database processing performed by the 1st information processor is enabled.

[0018]A network system concerning this invention Are an above-mentioned network system and a program is enciphered and recorded on the 1st recording medium and the 2nd information processor the 1st -- an information processor -- by transmitting information for decoding a program in the 1st enciphered recording medium reading processing of the 1st recording medium by the 1st information processor is made possible.

[0019]A network system concerning this invention is an above-mentioned network system and information for decoding is a key for decryption.

[0020]A network system concerning this invention The 2nd recording medium that is an above-mentioned network system and is different from the 1st recording medium further. It is connected to the 3rd information processor (for example other entertainment devices) with which it is equipped by (for example optical disc) and with the 2nd information processor. After receiving peculiar information relevant to the 1st recording medium from the 1st information processor peculiar information



relevant to the 2nd recording medium is received from the 3rd information processor.

[0021]A network system concerning this inventionAre an above-mentioned network system and further with the 2nd information processor. Peculiar information relevant to the 1st recording medium received from the 1st information processorit was referred to with reference to peculiar information relevant to the 2nd recording medium received from the 3rd information processor -- each -- when peculiar information overlapsreading processing of a program recorded on the 2nd recording medium performed in the 3rd information processor is made possible or impossible.

[0022]A network system concerning this invention is an above-mentioned network systemand the 2nd information processor makes possible executive operation of the 2nd recording medium performed in the 3rd information processor to the 1st information processoror transmits confirmed information about no.

[0023]A network system concerning this invention is an above-mentioned network systemand when there is consent from the 1st information processorit makes executive operation of the 2nd recording medium possible in the 3rd information processor.

[0024]A network system concerning this inventionTo the 1st information processorare an above-mentioned network systemand wearing of the 3rd recording medium (for examplememory card) is still enabledand the 2nd information processorafter receiving peculiar information relevant to the 1st information processor received from the 1st information processorand peculiar information relevant to the 1st recording medium -- each -- transmitting peculiar information to the 1st information processor -- the 1st information processor -- each -- peculiar information is accumulated into the 2nd recording medium.

[0025]A network system concerning this invention is an above-mentioned network systemand refer to peculiar information relevant to the 1st recording mediumand the information accumulated into the 3rd recording medium for the 1st information processor further.

[0026]A network system concerning this inventionIt is an above-mentioned network systemand when information applicable to peculiar information relevant to the 1st recording medium is accumulated into the 3rd recording medium as a result of reference by the 1st information processorprocessing performed by the 1st information processor is enabled.

[0027]A network system concerning this invention is an above-mentioned network systemand peculiar information relevant to an information processor is apparatus ID.

[0028]A network system concerning this invention is an above-mentioned network systemand peculiar information relevant to an information processor is user ID.

[0029]A network system concerning this invention is an above-mentioned network systemand peculiar information relevant to said recording medium is recording-medium ID.

[0030]A network system concerning this invention is an above-mentioned network

system a recording medium which recorded said application is an optical disc and said recording-medium ID is disk ID.

[0031] A network system concerning this invention is an above-mentioned network system and said disk ID is recorded on a field in a data area of said optical disc or fields other than a data area.

[0032] A network system concerning this invention is an above-mentioned network system and said disk ID is detected in said computer based on an address of disk ID information recorded on a data area of said optical disc.

[0033] A network system concerning this invention is an above-mentioned network system and said disk ID is recorded on a disk with organic coloring matter.

[0034] A network system concerning this invention is an above-mentioned network system and said disk ID is formed by a method using a physical change of a pit sequence.

[0035] A network system concerning this invention is an above-mentioned network system and a method using a physical change of said pit sequence uses either change of a radial direction of a pit sequence, change of the direction of a minor axis of pit size or change of a depth direction of a pit.

[0036] A network system concerning this invention is an above-mentioned network system and said disk ID is formed by a method using digital watermarking.

[0037] A method of attesting a recording medium concerning this invention: A network system which has the 1st information processor with which it is equipped with the 1st recording medium and the 1st information processor and the 2nd information processor connected via a network is used. A step to which it is the method of attesting this recording medium and the 2nd information processor receives peculiar information relevant to the 1st information processor and peculiar information relevant to the 1st recording medium from said 1st information processor. The 2nd information processor is connected or contained in the 2nd information processor and a step which attests a recording medium by referring to information in a database in which accumulation, elimination, etc. of information are possible and each received peculiar information is included.

[0038] The 1st information processor concerning this invention is the 1st information processor with which it is equipped with the 1st recording medium. Are the 2nd information processor and the 1st information processor connected via a network and this 1st information processor. Information in a database which transmits peculiar information relevant to the 1st information processor and peculiar information relevant to the 1st recording medium to said 2nd information processor and is connected or contained in the 2nd information processor and in which accumulation, elimination, etc. of information are possible. The 1st recording medium is attested by referring to each transmitted peculiar information.

[0039] The 2nd information processor concerning this invention is the 1st information processor with which it is equipped with the 1st recording medium and the 2nd information processor connected via a network. Peculiar information relevant to the 1st information processor in this 2nd information processor. Peculiar information relevant to the 1st recording medium is received from said 1st

information processor it is connected or contained in the 2nd information processor and the 1st recording medium is attested by referring to information in a database in which accumulation, elimination, etc. of information are possible and each received peculiar information.

[0040]. A recording medium concerning this invention is performed with the 1st information processor with which it is equipped with the 1st recording medium and the 2nd information processor connected via a network. With this 2nd information processor are a program which can be executed [ that reading is possible and ] the recorded recording medium and this program a step which receives peculiar information relevant to the 1st information processor and peculiar information relevant to the 1st recording medium from said 1st information processor. It is connected or contained in the 2nd information processor and a step which attests the 1st recording medium by referring to information in a database in which accumulation, elimination, etc. of information are possible and each received peculiar information is included.

[0041] A program concerning this invention is the 1st information processor with which it is equipped with the 1st recording medium. Perform with the 2nd information processor and the 1st information processor connected via a network. With this 1st information processor are a program which can be executed [ that reading is possible and ] the recorded recording medium and this program a step which transmits peculiar information relevant to the 1st information processor and peculiar information relevant to the 1st recording medium to said 2nd information processor. It is connected or contained in the 2nd information processor and a step which attests the 1st recording medium by referring to information in a database in which accumulation, elimination, etc. of information are possible and each transmitted peculiar information is included.

[0042]. A program concerning this invention is executed with the 1st information processor with which it is equipped with the 1st recording medium and the 2nd information processor connected via a network. With this 2nd information processor are a program which can be executed [ that reading is possible and ] and this program a step which receives peculiar information relevant to the 1st information processor and peculiar information relevant to the 1st recording medium from said 1st information processor. It is connected or contained in the 2nd information processor and a step which attests the 1st recording medium by referring to information in a database in which accumulation, elimination, etc. of information are possible and each received peculiar information is included.

[0043] A program concerning this invention is the 1st information processor with which it is equipped with the 1st recording medium. Perform with the 2nd information processor and the 1st information processor connected via a network. With this 1st information processor are a program which can be executed [ that reading is possible and ] and this program a step which transmits peculiar information relevant to the 1st information processor and peculiar information relevant to the 1st recording medium to said 2nd information processor. It is connected or contained in the 2nd information processor and a step which attests

the 1st recording medium by referring to information in a database in which accumulation, elimination, etc. of information are possible and each transmitted peculiar information is included.

[0044]

[Embodiment of the Invention] Hereafter this embodiment is described in detail referring to an attached drawing.

[Disk authentication system]

(Whole system) Drawing 1 is a key map of the whole disk authentication system concerning this example. As shown in drawing 1 the user terminal apparatus 1 is connected with the server 4 for attestation via the network 3. This server 4 for attestation is connected with 1 or the two or more contents servers 6 via the network 3. There may be the debugging dedicated server 6-4 in these contents servers 6.

[0045] The user terminal apparatus 1 is a computer which can carry the optical discs 2 which recorded the application programs such as CD-ROM (Compact Disc-ReadOnly Memory) and DVD-ROM (Digital Versatile Disc-ROM). This example explains taking the case of the entertainment system represented by the game machine etc. This user terminal apparatus 1 corresponds to the entertainment main frame and explains the composition of that inside about the entertainment main frame later using drawing 2. The optical disc 2 is illustration and is not limited to this. All various recording media that recorded contents such as an application program should consent to an object. For example these are applicable when contents such as an application program are recorded on the memory in the memory card connected to the hard disk (not shown) of external connection and the below-mentioned connector or PDA etc. However in order to explain plainly it explains taking the case of the optical disc 2.

[0046] As the network 3 what is called broadband network such as a television cable network, an optical fiber network and xDSL (x Digital Subscriber Line) are preferred. The broadband wireless network and cellular phone which will be built existing or from now on and a PHS (Personal Handyphone System) telephone-related network, an Internet related network etc. can be used.

[0047] It is connected to the entertainment device 1 and the server 4 for attestation has the entertainment device 1 and the genuine recording medium 2 or is a server used in order to perform that unjust attestation. The peculiar apparatus ID (it is also called "SET ID".) information which is ID that the server 4 for attestation was given to each entertainment main frame 1. The user ID (it is also called "USER ID".) information (a password may be included.) which is peculiar ID given to each user. It has the user databases 5 which accumulate User Information such as disk ID (it is also called "DISK ID".) which is peculiar ID given to each optical disc 2. These ID is respectively single and two or more same ID does not exist. Especially disk ID is the different classification symbol attached for every one optical disc.

[0048] The contents server 6 has the database 7 which accumulated various digital contents with which a user can be provided respectively.

[0049]The entertainment device 1 can also be used instead of the server 4 for attestation. That is it is a case where two or more entertainment devices 1 are connected and specific one of it plays the role of the server for attestation. In this case the user databases 5 connected to this comprise a recording medium like a hard disk.

[0050](Internal configuration of a device main frame) Drawing 2 is a block diagram of the internal configuration of the main frame of the entertainment system used as a user terminal of drawing 1. The inside of a figure and the inside of a dashed dotted line show the entertainment main frame 1 and the inside of a dashed line shows the disk drive 30 of this entertainment main frame 1 respectively.

[0051]The entertainment main frame 1 has CPU16 and this CPU16 is connected with the main memory (RAM) 17. CPU16 is connected with the drawing device (GPU) 18 and the video signal from GPU18 is outputted to the display (CRT) (not shown) via CRT-CTR (Cathode Ray Tube-Control) (not shown). Via IOP (Input/Output Processor) 13 which has the USB (Universal Serial Bus) connector 14 IEEE1394 or i link (i.LINK (registered trademark)) connector 15 grade CPU16 It is connected to the connector (a controller (PAD) / PDA (Personal Digital Assistant) / memory card connector) 12.

[0052]The memory card 11 the controller (PAD) 10 a personal digital assistant (PDA: Personal Digital Assistant) etc. are connected to this connector 12. This memory card 11 PDA etc. are kinds of an external storage and disk ID apparatus ID etc. are recorded so that it may mention later.

[0053]Via IOP13 CPU16 is connected to the bus 27 and in this bus 27. MASK-ROM (Masked ROM) 19 CD/DVD-DSP (CD/DVD-Digital Signal Processor) 22 DVD player ROM 20 SPU (Sound Processing) Unit 25 and network interface 26 grade are connected. The audio signal from SPU25 is outputted to amplifier a loudspeaker (not shown) etc. It is connected with a network via the network interface 26 USB connector 14 and i link connector 15 grade and also the entertainment main frame 1 is connected to the server 4 for attestation and digital contents server 6 grade through a network.

[0054]CD/DVD-DSP22 performs mechanical control of the disk drive 30 via the mechanical control section 23 and the driver 24. This control is performed through RF-AMP (Radio Frequency Amplifier) 21. CD/DVD-DSP22 performs electric control of the disk drive 30 through RF-AMP21.

[0055]The optical disc 2 rotates by mechanical control of a spindle motor (not shown). To the optical disc 2 a pickup lens (not shown) drives by electric control of an actuator (not shown) and record/playback of information are performed.

[0056]This entertainment device 1 has apparatus ID which is peculiar IDs such as a serial number. What was read from the thing incorporated in hardware so that it might be beforehand written for example in the mask ROM 19 or after by software via the optical disc 2 memory card 11 personal digital assistant and controller 10 grade and \*\*\*\*\* may be sufficient as this apparatus ID.

[0057]Disk ID is recorded on this optical disc 2 and this disk ID is read by the method of mentioning later.

[Disk ID authentication system]

(1st disk ID authentication system) Hereafter the processing by the side of the entertainment main frame of the 1st disk ID authentication system is concretely explained using drawing 3 and the processing by the side of the server 4 for attestation is concretely explained using drawing 4. In this example an entertainment system is a game machine. The case where an optical disc like CD-ROM is used as a recording medium which memorized the game program and also disk ID exists in area (for example the inside of read-in area, the outside of lead-out etc.) other than the usual data area is explained as a premise.

[0058] Drawing 3 shows the processing by the side of the entertainment main frame. First the foundations of the processing in the entertainment main frame are explained. Disk ID is recorded on the area where the optical disc currently used here does not serve as a recording object in usual. The information (for example address) which pinpoints the recording part of this disk ID is recorded on the usual data area. As a material for entering disk ID in the optical disc 2 the organic coloring matter currently used for the added type disk of a postscript is mentioned as an example. The entertainment main frame reads disk information, searched the address with which disk ID was recorded from there, reads disk ID according to this address further and has transmitted it to the server 4 for attestation. Hereafter it explains concretely.

[0059] In Step S102 the entertainment main frame 1 reads the basic data of TOC (Table of Contents) from the basis of control of CPU and carried CD-ROM. And in Step S103 the volume identifier VD (Volume Description) of the data area of CD-ROM is read and the address as which disk ID is filled in is searched.

[0060] In Step S104 it is judged whether the address of disk ID exists in the volume identifier VD. If the address of ID does not exist, carried CD-ROM is judged to be CD-ROMs other than the subject of protection by this disk ID authentication system; it goes on to Step S113 and a program is executed. This entertainment main frame 1 not only functions as a game machine but functions as the CD reproduction device for music, a DVD reproducer for movies etc. For this reason optical discs (for example DVD-Video, Audio-CD, the conventional game CD etc.) other than the subject of protection by an ID authentication system may be carried in the entertainment main frame and as for such a case music playback of an image and execution of a game are performed as it is.

[0061] When ID address exists in the volume identifier VD in order to read disk ID in Step S105 the pickup of the optical disk drive 30 is turned to the disk ID information part (portion provided in the read-in-area inside or the outside of lead-out) of CD-ROM and is made to slide according to ID address. Slide-controlling of this pickup is performed by the mechanical control section 23 based on the slide command outputted from CPU 16.

[0062] In Step S106 CPU 16 distinguishes whether disk ID information actually exists in the disk ID information part on CD-ROM. When disk ID information does not exist or when the read-in of disk ID information is impossible it is judged with having no disk ID and progresses to Step S107. In this step S107 execution of a

program is refused and forced to terminate.

[0063]When disk ID information actually exists in a disk ID information part in Step S108 under control of CPU16 of the entertainment main frame 1 reads disk ID information and memorizes this to the main memory 17.

[0064]In Step S109 CPU16 of the entertainment main frame 1 transmits the data of disk ID to the server 4 via the various communication interfaces based on the standard of IEEE1394, PCMCIA (Personal Computer Memory Card International Association Architecture) etc. It transmits to the server 4 for attestation. And it waits for the server for attestation to perform authenticating processing at Step S110 to disk ID which is transmitted.

[0065]In Step S111 the entertainment main frame 1 receives the authenticating processing result in the server for attestation. If the result of the authenticating processing in the server for attestation is "\*\*\*\*\*" the reading permission command of CD-ROM will be received. If the result of authenticating processing is "attestation no" it will progress to Step S112 and execution of a program is refused and forced to terminate.

[0066]When the result of the authenticating processing in the server for attestation is "\*\*\*\*\*" in Step S113 CPU of the entertainment main frame 1 executes the program recorded on CD-ROM.

[0067] Drawing 4 shows the processing by the side of the server 4 for attestation in the 1st disk ID authentication system. First the foundations of the processing in the server 4 for attestation are explained. The user who purchased the entertainment main frame 1 has registered into the user databases 5 of the server 4 for attestation user IDs such as his name and apparatus ID given to each body of equipment just behind that. If the user who purchased a new game program does not transmit disk ID information to the user databases 5 of the server 4 for attestation at the time of the first use he cannot do execution of the program (step S109 reference). For this reason disk ID and what has still more arbitrary user ID relevant to this apparatus ID etc. are accumulated in the user databases 5 of the server 4 for attestation at least as User Information. User Information will serve as combination of two or more disk ID to one user ID and apparatus ID if a user purchases the game program of two or more kinds. User Information is table-ized and is accumulated in the user databases 5.

[0068]Under such a situation when a user starts a game the information on disk ID which the user is using and apparatus ID is transmitted to the server 4 for attestation from the entertainment body equipment 1 and it is compared with User Information accumulated in the user databases of the server 4 for attestation. This comparison result will be the following four kinds as shown in drawing 7.

[0069](No.1) Both disk ID and apparatus ID are in agreement with what was accumulated.

[0070](No.2) Only disk ID is in agreement with what was accumulated.

[0071](No.3) Only apparatus ID is in agreement with what was accumulated.

[0072](No.4) Neither disk ID nor apparatus ID of what was accumulated corresponds.

[0073]When the combination of disk ID to which No.1 was transmitted and apparatus ID is in agreement with the information corresponding to these which were already registered into user databases this disk is judged to be a regular disk. However a case as apparatus ID is copied unjustly and disk ID was also unjustly copied as a rare case may happen. In order to eliminate such a case when the authentication demand of the same combination of disk ID and apparatus ID overlaps with the same time zone it judges that it is an unauthorized use counts this unauthorized use and records on the user databases 5 and execution of a program is refused.

[0074]When only disk ID is in agreement with what was accumulated in the database among the combination of disk ID to which No.2 was transmitted and apparatus ID three kinds of situations as follows can be considered.

[0075](1) To any of these when a disk owner lends his own disk to others and (2) disk owners perform their own disk by others' apparatus in (3) illegal copies it corresponds. It can distinguish by asking for a check the user of apparatus ID registered with disk ID. Such confirmation work of this entertainment system becomes possible by connecting each entertainment main frame 1 to the server 4 for attestation.

[0076]When disk ID is unregistered among the combination of disk ID to which No.3 and No.4 were transmitted and apparatus ID it is judged as first time use of the disk 2 and disk ID is registered into the user databases 5. It explains concretely below.

[0077]In Step S202 the server 4 for attestation performs connection authorization to the entertainment main frame 1 which a user uses. Here if apparatus ID of the main frame 1 is automatically supplied to a server as some send data from the main frame 1 the user should enter only the password which is user ID. When connection authorization goes wrong in Step S203 the connection between installed user terminals and the server 4 for attestation is intercepted. If connection authorization is successful in Step S204 a communication interface with a user's main frame 1 will be established.

[0078]In Step S205 the server 4 for attestation receives disk ID information and apparatus ID from the entertainment main frame 1. This is processing corresponding to Step S109 of drawing 3.

[0079]In Step S206 the server 4 for attestation performs comparison with disk ID and apparatus ID which received and User Information (disk ID apparatus ID) currently recorded on the user databases 5.

[0080]In Step S207 it is judged whether disk ID which received is in agreement with disk ID registered into the database 5. That is if there is no disk ID which received in the table on the user databases 5 the disk will be first-time use. In this case it progresses to Step S208 and the server 4 for attestation registers disk ID to the database 5. And a program execution permission command is transmitted to the entertainment main frame 1 at Step S212.

[0081]If transmitting disk ID is registered in the database 5 it will progress to Step S209 and it will be judged whether receiver ID and apparatus ID registered as a



use device of said disk ID are in agreement. When apparatus ID is inharmoniousit progresses to Step S210 and licence is checked to the user (disk owner) of apparatus ID corresponding to disk ID. If a disk owner consents at Step S211 (that isa disk owner) If it replies permitting disk use to the server 4this will be whether the disk owner lent his own disk to othersor to perform using other entertainment main frames 1and will be Step S212A program execution permission command is transmitted to the entertainment main frame 1.

[0082]When a disk owner does not consentit is judged as an unauthorized use the count of an unauthorized use is made at Step S214and a program execution refusal command is transmitted to the entertainment main frame at Step S215. Therebythe unauthorized use of a used article etc. is eliminated.

[0083]When it is a very rare case even when the combination of disk ID and apparatus ID is in agreement with User Information registered into the user databases 5but both ID is copied unjustlyit is necessary to eliminate this. It is judged whether at Step S213use in the combination of the same disk ID—apparatus ID as the same time zone overlaps. When concurrent use has not occurred a program execution permission command is transmitted to the entertainment main frame 1 at Step S212. When concurrent use has occurredit is judged as an unauthorized use the count of an unauthorized use is made at Step S214and a program execution refusal command is transmitted to the entertainment main frame at Step S215.

[0084]Usuallysince an inaccurate disk copies the genuine contents of a disk as it is the address information of disk ID recorded on the data area will also be copied. Howeverthe ID information recorded in addition to data areassuch as the inside of read in area in the format of this embodiment or the outside of read out area is not copied to the inaccurate disk which copied the genuine disk as it was. Since disk ID itself does not exist by this in spite of copying the information about the address of disk ID to the inaccurate disk an inaccurate disk is receivedExecution of a program will be eliminated at Step S107 by being judged with those of disk ID with an address at Step S104 of drawing 3and subsequently being judged with disk ID itself being nothing at Step S106.

[0085]The record method of disk ID is not limited to an above-mentioned method. For example disk ID can also be formed by the method using a physical change of the pit sequence in a data area. The method using a physical change of this pit sequence can use either change (wobbling) of the radial direction of a pit sequencechange of the direction of a minor axis of pit size or change of the depth direction of a pit. Or disk ID can also be formed by the method using digital watermarking (Digital Watermark).

[0086]The registration method of disk ID to the server for attestation is not limited to an above-mentioned method. There is a case so that the donor of recording mediasuch as an optical discitself may provide the server 4 for attestationfor example as a case of being special. In this casemanufacture and disk ID to provide can be registered and accumulated beforehand themselves at the database 5 of the server 4 for attestation. In such a casein the 1st disk ID

authentication system the registration processing of disk ID at the time of first time use becomes unnecessary.

[0087] Apparatus ID is not necessarily required. Apparatus ID can be replaced by user ID peculiar to each user. That is instead of specifying a use device a user can be specified and an authentication system can be operated with the combination of user ID and disk ID. In this case user ID is preferably given in the form of a password.

[0088] A case so that the donor of recording media such as an optical disc itself may provide the server 4 for attestation is explained.

[0089] This recording-medium donor gives an individual serial number for every one disk and incorporates as information in the disk 2 by setting this to disk ID at the time of disk manufacture. Simultaneously the disk ID (serial number) is recorded on the user databases 5. On the other hand at the time of manufacture of the entertainment device 1 an individual serial number is given for every one entertainment device and this is incorporated as apparatus ID in the entertainment device. And the apparatus ID (serial number) is simultaneously recorded on the user databases 5.

[0090] In this case at the time of the factory shipments of the disk 2 disk ID is not yet related with apparatus ID of the entertainment device 1.

[0091] The server 4 for attestation attests disk ID with the user of the disk 2 demanding connection and authenticating processing from the server 4 for attestation (S109) after apparatus ID authentication.

[0092] Since apparatus ID and disk ID (User Information) are beforehand recorded on the user databases 5 the server 4 for attestation confirms whether apparatus ID-disk ID which received from the entertainment device 1 corresponds to User Information recorded on these user databases 5.

[0093] As a result when there is nothing applicable to User Information of the user databases 5 attestation is forced to terminate and the program execution of the disk 2 is refused. Under the present circumstances if inaccurate disk ID is accumulated in the user databases 5 it becomes manageable with respect to inaccurate disks such as a count of the access frequency to the server 4 for attestation using the inaccurate disk for every entertainment device and specification using an inaccurate disk of the entertainment device 1.

[0094] The count of access frequency using the disk 2 with which disk ID was given also [ except exclusion of an inaccurate disk ] can be effectively used in the network system of this invention. That is when it reaches using the access frequency to the server 4 for attestation more than the number of times with access frequency attestation is forced to terminate and the program execution of the disk 2 can be refused.

[0095] For example it is possible to provide a trial period to contents such as a program included in the disk 2 and to make a user use by managing the access frequency to the server 4 for attestation using the disk 2 with which ID was given. Thereby a user can use a game service etc. as a trial period using contents such as a program in a disk until he becomes a fixed count with the using frequency of a

certain disk 2.

[0096]Now although many Internet access service trial version software has provided the trial period at counting the utilization time if the network system of this invention is used it will become manageable according to not the management by the utilization time of service but using frequency.

[0097]For example it is available in the service which makes download offer of music or the image from the contents server 6 to the entertainment device 1 via the server 4 for attestation of this invention. Here the disk 2 for service use shall be distributed to the user who joined service from a purveyor of service. In the disk the program for attestation the program for download execution etc. are recorded with disk ID given for every disk. By equipping the entertainment device 1 with this disk 2 a user becomes possible [ connecting with the server 4 for attestation and the contents server 6 ] and thereby becomes downloadable about music an image etc.

[0098]Under the present circumstances if the server 4 for attestation counts download frequency as access frequency to the contents server 6 using the disk 2 which gave disk ID realization of using frequency restrictions of service will be attained [ that it is not dependent on download (communication) time and ].

[0099]If the information and User Information showing the contents of contents which the user accessed in the server 4 for attestation (apparatus ID user ID disk ID etc.) are associated mutually and it accumulates into the user databases 5 it will become possible to manage the taste for every user etc. easily. A purveyor of service or a contents provider becomes possible [ providing a suitable advertisement etc. through communication lines such as the Internet for every user ] using such accumulation information.

[0100]Although the above was use limiting methods according to using frequency such as service provision a limiting method is not restricted to this. For example according to the \*\*\*\* situation from a user a purveyor of service can impose restriction and can also provide the contents recorded on the disk 2 with which disk ID was given. The contents recorded on the disk 2 make all available that it is not available and selectively. When a user wants to use the contents whose use is selectively impossible a user will pay a purveyor of service the remuneration according to the contents of use. A purveyor of service enables use by a user in response to it.

[0101]For example if the contents recorded on the disk 2 are enciphered selectively the user who does not pay a use remuneration receives the user equivalent to a code portion who paid the use remuneration although it could not use. By providing for a user's entertainment device 1 it becomes available from a purveyor of service about the key for decoding a code. The information transmitted from said purveyor of service to the entertainment device 1 is not restricted to the key for decryption.

[0102]It may be the transmission of user ID to the server 4 for attestation which it is not restricted to the payment of a remuneration for example a purveyor of service manages from a user's entertainment device 1 which is performed to a

purveyor of service in order that a user may use the contents of record which cannot use the disk 2 selectively. This user ID may be ID beforehand given from the purveyor of service to each user.

[0103](The 2nd disk ID authentication system)next the 2nd disk ID authentication system are explained. In the 2nd disk ID authentication systemthe disk used as the candidate for attestation is not limited to CD-ROM etc.but DVD-ROM etc. with which TOC is not specified are included. The recording part of disk ID in a disk may not be limitedeitherbut they may be the inside of read in areathe outside of lead-outor which part in a data area.

[0104]In order to play a game by the 1st disk authentication system as compared with the disk authentication system of the above 1stwhenever it started the program on a diskwere attesting by connecting with a serverbut. At this 2nd disk authentication systemthe processing distance linked to a server is omitted by memorizing User Information to the main part connection type external storage of memory card 11 grade. Namelyat the time of first time use of a diskUser Information of disk ID-apparatus ID is recorded on memory card 11 gradeand the disk is attested for every game execution using this User Information.

Contentssuch as an application programmay be recorded on the external storage.

[0105]The processing by the side of the entertainment main frame of the 2nd disk ID authentication system is concretely explained using drawing 5and the contents of processing in each step by the side of the server 4 for attestation are concretely explained using drawing 6.

[0106]By SUTE@PPU S302the entertainment main frame 1 reads into the main memory 17 the peculiar basic data currently recorded on the wearing disk 2 under control of CPU16. As for the wearing disk 2various diskssuch as CDCD-ROMDVD-Videoand DVD-ROMare contained.

[0107]In Step S303it is judged whether disk ID is in the read basic data. If disk ID does not existit is judged that they are disks other than for attestationit progresses to Step S312and a program is executed.

[0108]When disk ID existsit progresses to Step S304 and User Information (combination data of disk ID-apparatus ID) recorded on the external storage of the memory card 11 grade connected to the entertainment main frame is read under control of CPU16. The data of the high-speed-steel core of a gamethe backup data of the advancing state of a game interrupted last timeetc. is also recorded on this memory card 11 grade.

[0109]In Step S305it is judged whether disk ID is recorded on the memory card 11. Since disk ID and apparatus ID are registered into User Information of the memory card 11 when a disk is used firstat the time of use of the 2nd henceforthdisk ID will be recorded on the memory card 11 as User Information. Thereforeas a case where there is no record of disk ID in the memory card 11the time of exchange of the \*\* memory card itselfetc. can be considered at the time of first time use of \*\* disk. When read disk ID is recorded on the memory card etc.it progresses to Step S306.

[0110]In Step S306it is judged whether disk ID currently recorded on the memory

card 11 grade is in agreement with disk ID of a wearing disk. As a case of not being in agreement others can be considered at the time of first time use of a disk. If in agreement it will progress to Step S307.

[0111] In Step S307 it is judged whether apparatus ID read from the memory card 11 is in agreement with apparatus ID of the main frame used now. The case where the user who borrows the disk 2 and the memory card 11 from a disk owner plays a game with his main frame as a case of not being in agreement etc. can be considered. When in agreement it corresponds to just use (when the combination of disk ID–apparatus ID is in agreement with User Information recorded on the memory card etc. at the time of disk purchase) user authentication is completed and a program is executed at Step S312.

[0112] When disk ID does not exist in a memory card at Step S305 at Step S306. When disk ID currently recorded on the memory card 11 grade is not in agreement with disk ID read from the disk or when apparatus ID currently recorded on the memory card 11 grade is not in agreement with apparatus ID of a use device at Step S307 it progresses to Step S308. At this step S308 the entertainment main frame transmits disk ID and the apparatus ID information of a use device to the server 4 for attestation via the communication interface of USB IEEE1394 PCMCIA etc. and it waits for user authentication at Step S309.

Then these writing is performed when the command which records these disk ID and apparatus ID information on the memory card 11 is received from the server 4 for attestation (it corresponds to Step S405 of drawing 6).

[0113] At Step S310 the propriety of the execution of the authenticating processing result in the server 4 for attestation of a program to origin is determined. In the case of “attestation no” it progresses to Step S311 and execution of a program is refused and forced to terminate. In “\*\*\*\*\*” it progresses to Step S312 and a program is executed.

[0114] Drawing 6 shows the contents of processing by the side of the server 4 for attestation in the 2nd disk ID authentication system.

[0115] At Step S402 the server 4 for attestation receives disk ID and apparatus ID of the main frame after establishing the connection to the entertainment main frame. It is disk ID which disk ID was read in the disk at Step S302 of drawing 5 and was transmitted at Step S308 and apparatus ID is also transmitted at Step S308.

[0116] It is judged whether at Step S403 disk ID which received exists in disk ID accumulated in the user databases of the server 4 for attestation. When it does not exist the disk is judged to be first time use. Therefore at Step S404 the combination of disk ID–apparatus ID which received table–izes to the user databases 5 as User Information and is accumulated in them (registration). Subsequently authenticating processing explained by drawing 5 is made possible by making it record on the memory card 11 grade which associates disk ID–apparatus ID mutually and is connected to a user’s main frame 1 at Step S405.

[0117] At Step S406 the server 4 for attestation transmits the password to the disk used to the main frame 1. This password is a secret key which only the owner of a

disk cannot know and it is used for a user's intention check so that it may mention later. As for this password it is preferred to be outputted to the screen of the main frame 1 which a user uses. A user teaches a password when lending out a disk to others by writing down this password and it becomes possible for those others to enable it to use a disk. Then a program execution permission command is transmitted to the entertainment main frame at Step S414.

[0118] When receiving disk ID is in agreement with disk ID registered at Step S403 at Step S407. It is compared whether apparatus ID which received is in agreement with apparatus ID in the database corresponding to said disk ID and it is judged whether both are in agreement at Step S408. Since the data which becomes the user databases 5 from the combination of disk ID-apparatus ID is stored about the disk used also at once in this step S408 apparatus ID distinguishes whether it is a thing corresponding to disk ID. Thereby used use can be eliminated. The server 4 for attestation transmits the combination data of disk ID-apparatus ID to the entertainment main frame and is made to record it on a memory card at Step S409 in exchange of the memory card 11 disappearance of record of disk ID-apparatus ID of a memory card etc. Then a program execution permission command is transmitted to the entertainment main frame at Step S414.

[0119] Although disk ID exists in the user databases 5 when correspondence apparatus ID is not in agreement with the thing in a database it progresses to Step S410 from Step S408 and the input request of a password is transmitted to the entertainment main frame 1. This input request is displayed on the television monitor (not shown) connected to the main frame 1. At Step S411 it is judged whether the password received from the user is just. If just it progresses to Step S412 and a new password will be published to the borrower of this disk etc. and it will transmit to them. When a disk borrower etc. borrow a disk from a disk owner under agreement it becomes possible in entering this password to avoid a program execution refusal command. As a result a disk borrower not necessarily loses his necessity of borrowing the memory card 11 with the disk 2 from a disk owner. In Step S412 the password peculiar to a disk published to the disk owner is updated. The updated password is transmitted to a disk owner. It is avoidable that this promotes spread of a used article.

[0120] The server 4 for attestation transmits a program execution permission command to the entertainment main frame at Step S414 after Step S412.

[0121] At Step S411 when it is judged that the password received from the user is not just it progresses to Step S413 and a program execution refusal command is transmitted from the server 4 for attestation to the entertainment main frame.

[0122] In the example of the 1st disk ID authentication system mentioned above and the 2nd disk ID authentication system the user has read the program from a recording medium like the optical disc which exists at hand to his own entertainment device 1. However this invention is not limited to this. For example the recording medium with which disk ID was given is in the other place and after performing the 1st or 2nd disk ID authentication system by remote control and obtaining attestation permission the program recorded on the recording

medium is also downloadable. Or after the recording medium with which disk ID was given for example downloads the program which is in the other place and was recorded on the recording medium the 1st or 2nd disk ID authentication system is performed attestation permission can be obtained and a program can also be executed.

[0123]

[Effect of the Invention] According to this invention the computer system which has an authentication system which verifies whether recording media such as an optical disc are used improperly can be provided.

[0124] According to this invention the directions for the computer system which has an authentication system which verifies whether recording media such as an optical disc are used improperly can be provided.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] Drawing 1 is a figure explaining a disk ID authentication system.

[Drawing 2] Drawing 2 is a figure showing the composition of the entertainment main frame of drawing 1.

[Drawing 3] Drawing 3 is a flow of processing by the side of the main frame in the 1st disk ID authentication method.

[Drawing 4] Drawing 4 is a flow of processing by the side of the server for attestation in the 1st disk ID authentication method.

[Drawing 5] Drawing 5 is a flow of processing by the side of the main frame in the 2nd disk ID authentication method.

[Drawing 6] Drawing 6 is a flow of processing by the side of the server for attestation in the 2nd disk ID authentication method.

[Drawing 7] Drawing 7 is a table showing the comparison result of disk ID and apparatus ID which the server for attestation received and User Information beforehand accumulated in user databases.

[Description of Notations]

- 1: Entertainment main frame (computer)
  - 2: Optical disc (the 1st recording medium)
  - 4: The server for attestation
  - 5: User databases
  - 6: Contents server
  - 7: Database
  - 11: Memory card (the 2nd recording medium)
-

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-334511

(P2002-334511A)

(43) 公開日 平成14年11月22日 (2002. 11. 22)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
G 1 1 B 20/10		G 1 1 B 20/10	D 5 B 0 1 7
			H 5 B 0 6 5
G 0 6 F 3/06	3 0 4	G 0 6 F 3/06	3 0 4 H 5 D 0 4 4
12/14	3 2 0	12/14	3 2 0 F 5 D 0 9 0
G 1 1 B 7/004		G 1 1 B 7/004	C 5 D 1 1 0
審査請求 有 請求項の数38 O L (全 18 頁) 最終頁に続く			

(21) 出願番号 特願2002-22360 (P2002-22360)

(22) 出願日 平成14年1月30日 (2002. 1. 30)

(31) 優先権主張番号 特願2001-22811 (P2001-22811)

(32) 優先日 平成13年1月31日 (2001. 1. 31)

(33) 優先権主張国 日本 (J P)

(71) 出願人 395015319

株式会社ソニー・コンピュータエンタテインメント

東京都港区赤坂7-1-1

(72) 発明者 久夢良木 健

東京都港区赤坂7丁目1番1号 株式会社  
ソニー・コンピュータエンタテインメント  
内

(74) 代理人 100101867

弁理士 山本 寿武

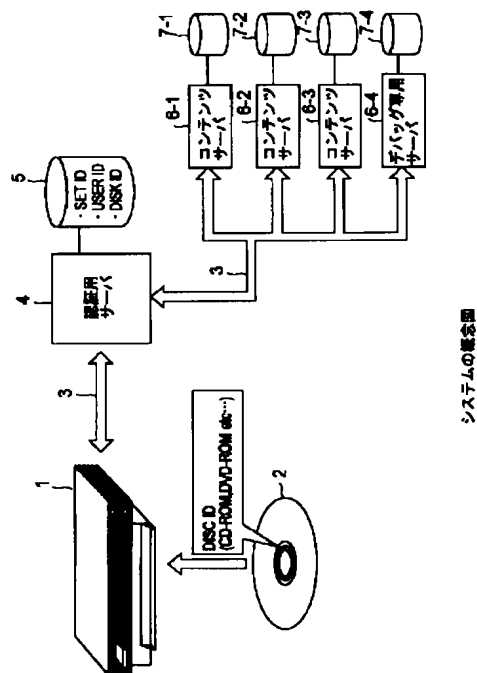
最終頁に続く

(54) 【発明の名称】 コンピュータシステム及びその使用方法

(57) 【要約】

【課題】 光ディスクが不正使用されているか否かを検証する認証システムを有するコンピュータシステム

【解決手段】 光ディスクが夫々装着可能な複数のコンピュータがネットワークを介して認証用サーバに接続可能なコンピュータシステムであって、各々の前記コンピュータは固有の機器IDを有し、各々の前記光ディスクは固有のディスクIDを有し、前記サーバは、前記コンピュータの使用時に前記機器IDを、前記光ディスクの使用時にディスクIDを、夫々蓄積するユーザデータベースを有し、該ユーザデータベースにはディスクID-機器IDの組のデータが蓄積されており、前記光ディスクの2回目以降の使用時には、前記コンピュータから前記ネットワークを介してディスクIDデータと機器IDデータとを認証用サーバに送信し、正当な使用であることを認証する。





## 【特許請求の範囲】

【請求項1】 第1の記録媒体が装着される第1の情報処理装置と、  
第1の情報処理装置とネットワークを介して接続される第2の情報処理装置とを備えたネットワークシステムにおいて、

第2の情報処理装置は、

第1の情報処理装置に関連した固有の情報と、第1の記録媒体に関連した固有の情報とを前記第1の情報処理装置から受信し、

第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで記録媒体の認証を行う、ネットワークシステム。

【請求項2】 請求項1に記載のネットワークシステムにおいて、該ネットワークシステムは、更に、  
第2の情報処理装置によって、第1の情報処理装置或いは第1の記録媒体に関連した固有の情報をデータベース内に蓄積する、ネットワークシステム。

【請求項3】 請求項1に記載のネットワークシステムは、更に第2の情報処理装置によって、第1の情報処理装置及び第1の記録媒体に関連した固有の情報をデータベース内に蓄積する、ネットワークシステム。

【請求項4】 請求項1～3のいずれか一項に記載のネットワークシステムにおいて、  
データベース内の情報は、予め記録された前記第1の情報処理装置或いは第1の記録媒体に関連した固有の情報である、ネットワークシステム。

【請求項5】 請求項1～3のいずれか一項に記載のネットワークシステムにおいて、  
データベース内の情報は、予め記録された前記第1の情報処理装置及び第1の記録媒体に関連した固有の情報である、ネットワークシステム。

【請求項6】 請求項2又は請求項3に記載のネットワークシステムにおいて、  
データベース内の情報は、あらたに蓄積された情報に更新される、ネットワークシステム。

【請求項7】 請求項2～6のいずれか一項に記載のネットワークシステムにおいて、  
記録媒体が不正に使用された際に、第1の情報処理装置或いは第1の記録媒体に関連した固有の情報をデータベース内に蓄積する、ネットワークシステム。

【請求項8】 請求項1～7のいずれか一項に記載のネットワークシステムは、更に第2の情報処理装置によって、第1の情報処理装置において実行される処理を可能あるいは不可能とする、ネットワークシステム。

【請求項9】 請求項1～8のいずれか一項に記載のネットワークシステムは、更に第2の情報処理装置によって、第1の情報処理装置において実行される第1の記録媒体に記録されたプログラムの読取り処理を可能あるいは

不可能とする、ネットワークシステム。

【請求項10】 請求項8又は請求項9に記載のネットワークシステムにおいて、

第2の情報処理装置は、第1の情報処理装置によって実行されるべき処理を可能とする許可信号、あるいは、第1の情報処理装置によって実行されるべき処理を不可能とする拒否信号を送信する、ネットワークシステム。

【請求項11】 請求項10に記載のネットワークシステムにおいて、

第2の情報処理装置による参照の結果、データベース内に第1の記録媒体に関連した固有の情報に該当する情報が蓄積されている場合に、第1の情報処理装置によって実行される処理を可能とする、ネットワークシステム。

【請求項12】 請求項10に記載のネットワークシステムにおいて、

データベース内には第1の情報処理装置に関連した固有の情報及び第1の記録媒体に関連した固有の情報とが関連付けられた情報として蓄積され、

第2の情報処理装置による参照の結果、第2の情報処理装置が受信した前記第1の情報処理装置に関連した固有の情報及び第1の記録媒体に関連した固有の情報が、データベース内の関連付けられた情報と一致した場合には、第1の情報処理装置によって実行される処理を可能とする、ネットワークシステム。

【請求項13】 請求項9に記載のネットワークシステムにおいて、

第1の記録媒体にはプログラムが暗号化して記録され、第2の情報処理装置は、第1の情報処理装置によって暗号化された第1の記録媒体内のプログラムを解読するための情報を送信することで、第1の情報処理装置による第1の記録媒体の読取り処理を可能とする、ネットワークシステム。

【請求項14】 請求項13に記載のネットワークシステムにおいて、  
解読するための情報は、暗号解読用の鍵である、ネットワークシステム。

【請求項15】 請求項1～14のいずれか一項に記載のネットワークシステムは、更に第1の記録媒体とは異なる第2の記録媒体が装着される第3の情報処理装置に接続され、

第2の情報処理装置によって、第1の情報処理装置から第1の記録媒体に関連する固有の情報を受信すると共に、第3の情報処理装置から第2の記録媒体に関連した固有の情報を受信する、ネットワークシステム。

【請求項16】 請求項15に記載のネットワークシステムは、更に、

第2の情報処理装置によって、第1の情報処理装置から受信した第1の記録媒体に関連した固有の情報と、第3の情報処理装置から受信した第2の記録媒体に関連した固有の情報を参照し、参照した各固有の情報が重複し

た場合には、第3の情報処理装置において実行される第2の記録媒体に記録されたプログラムの読取り処理を可能あるいは不可能とする、ネットワークシステム。

【請求項17】 請求項16に記載のネットワークシステムは、更に第2の情報処理装置が、第1の情報処理装置に対して、第3の情報処理装置において行われる第2の記録媒体の実行処理を可能にするか否に関して確認情報を送信する、ネットワークシステム。

【請求項18】 請求項17に記載のネットワークシステムにおいて第2の情報処理装置が、第1の情報処理装置から承諾があった時、第3の情報処理装置において第2の記録媒体の実行処理を可能とする、ネットワークシステム。

【請求項19】 請求項1～18のいずれか一項に記載のネットワークシステムにおいて、第1の情報処理装置には更に第3の記録媒体が装着可能とされ、第2の情報処理装置は、第1の情報処理装置から受信した第1の情報処理装置に関連した固有の情報及び第1の記録媒体に関連した固有の情報を受信した後に、各固有の情報を第1の情報処理装置に対して送信し、第1の情報処理装置は各固有の情報を、第2の記録媒体内に蓄積する、ネットワークシステム。

【請求項20】 請求項19に記載のネットワークシステムにおいて、更に第1の情報処理装置は、第1の記録媒体に関連した固有の情報と、第3の記録媒体内に蓄積された情報とを参照する、ネットワークシステム。

【請求項21】 請求項20に記載のネットワークシステムにおいて、第1の情報処理装置による参照の結果、第3の記録媒体内に第1の記録媒体に関連する固有の情報に該当する情報が蓄積されている場合には、第1の情報処理装置によって実行される処理を可能とする、ネットワークシステム。

【請求項22】 請求項1～21のいずれか一項に記載の前記ネットワークシステムにおいて、情報処理装置に関連した固有の情報は機器IDである、ネットワークシステム。

【請求項23】 請求項1～22のいずれか一項に記載の前記ネットワークシステムにおいて、情報処理装置に関連した固有の情報はユーザIDである、ネットワークシステム。

【請求項24】 請求項1～22のいずれか一項に記載の前記ネットワークシステムにおいて、前記記録媒体に関連した固有の情報は記録媒体IDである、ネットワークシステム。

【請求項25】 請求項1に記載のコンピュータシステムにおいて、前記アプリケーションを記録した記録媒体が光ディスクであり、前記記録媒体IDがディスクIDである、コン

ピュータシステム。

【請求項26】 請求項25に記載のコンピュータシステムにおいて、前記ディスクIDは、前記光ディスクのデータエリア内の領域又はデータエリア以外の領域に記録されている、コンピュータシステム。

【請求項27】 請求項25に記載のコンピュータシステムにおいて、前記コンピュータでは、前記ディスクIDは、前記光ディスクのデータエリアに記録されたディスクIDデータのアドレスに基づき検出される、コンピュータシステム。

【請求項28】 請求項25に記載のコンピュータシステムにおいて、前記ディスクIDは、有機色素によりディスクに記録されている、コンピュータシステム。

【請求項29】 請求項25に記載のコンピュータシステムにおいて、前記ディスクIDは、ビット列の物理的な変動を利用した方法で形成されている、コンピュータシステム。

【請求項30】 請求項29に記載のコンピュータシステムにおいて、前記ビット列の物理的な変動を利用した方法は、ビット列の半径方向の変動、ビットサイズの短径方向の変動又はビットの深さ方向の変動のいずれかを利用している、コンピュータシステム。

【請求項31】 請求項25に記載のコンピュータシステムにおいて、前記ディスクIDは、電子透かしを利用した方法で形成されている、コンピュータシステム。

【請求項32】 第1の記録媒体が装着される第1の情報処理装置、第1の情報処理装置とネットワークを介して接続される第2の情報処理装置を有するネットワークシステムを利用して、該記録媒体の認証を行う方法において、

第2の情報処理装置が、前記第1の情報処理装置から、第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報とを受信するステップと、第2の情報処理装置が、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む、方法。

【請求項33】 第1の記録媒体が装着される第1の情報処理装置であって、第2の情報処理装置とネットワークを介して接続された第1の情報処理装置において、該第1の情報処理装置は、第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報とを、前記第2の情報処理装置に送信し、第2の情報処理装置に接続或いは含まれ、情報の蓄積・

消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第1の記録媒体の認証を行う、第1の情報処理装置。

【請求項34】 第1の記録媒体が装着される第1の情報処理装置とネットワークを介して接続される第2の情報処理装置において、該第2の情報処理装置は、第1の情報処理装置に関連した固有の情報と、第1の記録媒体に関連した固有の情報とを前記第1の情報処理装置から受信し、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第1の記録媒体の認証を行う、第2の情報処理装置。

【請求項35】 第1の記録媒体が装着される第1の情報処理装置とネットワークを介して接続される第2の情報処理装置で実行される、該第2の情報処理装置で読み取り可能且つ実行可能なプログラムを記録した記録媒体において、該プログラムは、第1の情報処理装置に関連した固有の情報と、第1の記録媒体に関連した固有の情報とを前記第1の情報処理装置から受信するステップと、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む、記録媒体。

【請求項36】 第1の記録媒体が装着される第1の情報処理装置であって、第2の情報処理装置とネットワークを介して接続された第1の情報処理装置で実行される、該第1の情報処理装置で読み取り可能且つ実行可能なプログラムを記録した記録媒体において、該プログラムは、第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報とを、前記第2の情報処理装置に送信するステップと、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む、記録媒体。

【請求項37】 第1の記録媒体が装着される第1の情報処理装置とネットワークを介して接続される第2の情報処理装置で実行される、該第2の情報処理装置で読み取り可能且つ実行可能なプログラムにおいて、第1の情報処理装置に関連した固有の情報と、第1の記録媒体に関連した固有の情報とを前記第1の情報処理装置から受信するステップと、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む、プログラム。

【請求項38】 第1の記録媒体が装着される第1の情

報処理装置であって、第2の情報処理装置とネットワークを介して接続された第1の情報処理装置で実行される、該第1の情報処理装置で読み取り可能且つ実行可能なプログラムにおいて、

第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報とを、前記第2の情報処理装置に送信するステップと、

第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む、プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムに関する。

【0002】

【従来の技術】 光ディスクを装着して使用するコンピュータでは、各種のプログラムを実行することが出来る。このようなコンピュータの一つにエンタテインメントシステムがあり、代表的にはゲーム装置として使用されている。このようなエンタテインメントシステムでは、ゲームプログラムが記録された光ディスクを購入し、ゲームを実行する。また最近、エンタテインメントシステムは、ネットワークを介して、多数のゲームプログラムを蓄積したコンテンツサーバと接続され、ゲームプログラムをネットワークを介してダウンロードして購入するようなことも計画されている。

【0003】

【発明が解決しようとする課題】 購入された光ディスク又はダウンロードしたプログラムを記録した光ディスクが、不正に使用される場合がある。即ち、プログラムを記録した光ディスクが、プログラムに関する著作権者の許可無く、不正にコピーされたり、これを中古品として販売されたりすることがある。このような状態を放置すると、著作権者は正当な利益を回収することが出来ず、プログラム創作の意欲が削がれることになる。

【0004】

【課題を解決するための手段】 上述の問題点に鑑みて、本発明は、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムを有するコンピュータシステムを提供することを目的とする。

【0005】 更に、本発明は、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムを有するコンピュータシステムの使用法を提供することを目的とする。

【0006】 本発明に係るネットワークシステムは、第1の記録媒体（例えば、光ディスク）が装着される第1の情報処理装置（例えば、一のエンタテインメント装置）と、第1の情報処理装置とネットワークを介して接続さ

れる第2の情報処理装置（例えば、認証用サーバ）とを備えたネットワークシステムであって、第2の情報処理装置は、第1の情報処理装置に関連した固有の情報（例えば、機器ID）と、第1の記録媒体に関連した固有の情報とを前記第1の情報処理装置から受信し、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで記録媒体の認証を行う。

【0007】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、該ネットワークシステムは、更に、第2の情報処理装置によって、第1の情報処理装置或いは第1の記録媒体に関連した固有の情報をデータベース内に蓄積する。

【0008】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第2の情報処理装置によって、第1の情報処理装置及び第1の記録媒体に関連した固有の情報をデータベース内に蓄積する。

【0009】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、データベース内の情報は、予め記録された前記第1の情報処理装置或いは第1の記録媒体に関連した固有の情報である。

【0010】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、データベース内の情報は、予め記録された前記第1の情報処理装置及び第1の記録媒体に関連した固有の情報である。

【0011】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、データベース内の情報は、あらたに蓄積された情報に更新される。

【0012】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、記録媒体が不正に使用された際に、第1の情報処理装置或いは第1の記録媒体に関連した固有の情報をデータベース内に蓄積する。

【0013】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第2の情報処理装置によって、第1の情報処理装置において実行される処理を可能あるいは不可能とする。

【0014】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第2の情報処理装置によって、第1の情報処理装置において実行される第1の記録媒体に記録されたプログラムの読取り処理を可能あるいは不可能とする。

【0015】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第2の情報処理装置は、第1の情報処理装置によって実行されるべき処理を可能とする許可信号、あるいは、第1の情報処理装置によって実行されるべき処理を不可能とする拒否信号を送信する。

【0016】更に、本発明に係るネットワークシステム

は、上述のネットワークシステムであって、第2の情報処理装置による参照の結果、データベース内に第1の記録媒体に関連した固有の情報に該当する情報が蓄積されている場合に、第1の情報処理装置によって実行される処理を可能とする。

【0017】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、データベース内には第1の情報処理装置に関連した固有の情報及び第1の記録媒体に関連した固有の情報とが関連付けられた情報として蓄積され、第2の情報処理装置による参照の結果、第2の情報処理装置が受信した前記第1の情報処理装置に関連した固有の情報及び第1の記録媒体に関連した固有の情報が、データベース内の関連付けられた情報と一致した場合には、第1の情報処理装置によって実行される処理を可能とする。

【0018】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第1の記録媒体にはプログラムが暗号化して記録され、第2の情報処理装置は、第1の情報処理装置によって暗号化された第1の記録媒体内のプログラムを解読するための情報を送信することで、第1の情報処理装置による第1の記録媒体の読取り処理を可能とする。

【0019】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、解読するための情報は、暗号解読用の鍵である。

【0020】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第1の記録媒体とは異なる第2の記録媒体（例えば、光ディスク）が装着される第3の情報処理装置（例えば、他のエンタテインメント装置）に接続され、第2の情報処理装置によって、第1の情報処理装置から第1の記録媒体に関連する固有の情報を受信した後に、第3の情報処理装置から第2の記録媒体に関連した固有の情報を受信する。

【0021】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第2の情報処理装置によって、第1の情報処理装置から受信した第1の記録媒体に関連した固有の情報と、第3の情報処理装置から受信した第2の記録媒体に関連した固有の情報とを参照し、参照した各固有の情報が重複した場合には、第3の情報処理装置において実行される第2の記録媒体に記録されたプログラムの読取り処理を可能あるいは不可能とする。

【0022】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第2の情報処理装置が、第1の情報処理装置に対して、第3の情報処理装置において行われる第2の記録媒体の実行処理を可能にするか否に関して確認情報を送信する。

【0023】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第1の情報

処理装置から承諾が有った時、第3の情報処理装置において第2の記録媒体の実行処理を可能とする。

【0024】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第1の情報処理装置には更に第3の記録媒体（例えば、メモリカード）が装着可能とされ、第2の情報処理装置は、第1の情報処理装置から受信した第1の情報処理装置に関連した固有の情報及び第1の記録媒体に関連した固有の情報を受信した後に、各固有の情報を第1の情報処理装置に対して送信し、第1の情報処理装置は各固有の情報を、第2の記録媒体内に蓄積する。

【0025】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第1の情報処理装置は、第1の記録媒体に関連した固有の情報と、第3の記録媒体内に蓄積された情報とを参照する。

【0026】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第1の情報処理装置による参照の結果、第3の記録媒体内に第1の記録媒体に関連する固有の情報に該当する情報が蓄積されている場合には、第1の情報処理装置によって実行される処理を可能とする。

【0027】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、情報処理装置に関連した固有の情報は機器IDである。

【0028】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、情報処理装置に関連した固有の情報はユーザIDである。

【0029】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記記録媒体に関連した固有の情報は記録媒体IDである。

【0030】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記アプリケーションを記録した記録媒体が光ディスクであり、前記記録媒体IDがディスクIDである。

【0031】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ディスクIDは、前記光ディスクのデータエリア内の領域又はデータエリア以外の領域に記録されている。

【0032】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記コンピュータでは、前記ディスクIDは、前記光ディスクのデータエリアに記録されたディスクIDデータのアドレスに基づき検出される。

【0033】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ディスクIDは、有機色素によりディスクに記録されている。

【0034】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ディスクIDは、ピット列の物理的な変動を利用した方法で形

成されている。

【0035】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ピット列の物理的な変動を利用した方法は、ピット列の半径方向の変動、ピットサイズの短径方向の変動又はピットの深さ方向の変動のいずれかを利用している。

【0036】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ディスクIDは、電子透かしを利用した方法で形成されている。

【0037】更に、本発明に係る記録媒体の認証を行う方法は、第1の記録媒体が装着される第1の情報処理装置、第1の情報処理装置とネットワークを介して接続される第2の情報処理装置を有するネットワークシステムを利用して、該記録媒体の認証を行う方法であって、第2の情報処理装置が、前記第1の情報処理装置から、第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報とを受信するステップと、第2の情報処理装置が、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで記録媒体の認証を行うステップとを含む。

【0038】更に、本発明に係る第1の情報処理装置は、第1の記録媒体が装着される第1の情報処理装置であり、第2の情報処理装置とネットワークを介して接続された第1の情報処理装置であって、該第1の情報処理装置は、第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報とを、前記第2の情報処理装置に送信し、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第1の記録媒体の認証を行う。

【0039】更に、本発明に係る第2の情報処理装置は、第1の記録媒体が装着される第1の情報処理装置とネットワークを介して接続される第2の情報処理装置であって、該第2の情報処理装置は、第1の情報処理装置に関連した固有の情報と、第1の記録媒体に関連した固有の情報とを前記第1の情報処理装置から受信し、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第1の記録媒体の認証を行う。

【0040】更に、本発明に係る記録媒体は、第1の記録媒体が装着される第1の情報処理装置とネットワークを介して接続される第2の情報処理装置で実行される、該第2の情報処理装置で読み取り可能且つ実行可能なプログラムを記録した記録媒体であって、該プログラムは、第1の情報処理装置に関連した固有の情報と、第1の記録媒体に関連した固有の情報とを前記第1の情報処理装置から受信するステップと、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータ

ベース内の情報と、受信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む。

【0041】更に、本発明に係るプログラムは、第1の記録媒体が装着される第1の情報処理装置であって、第2の情報処理装置とネットワークを介して接続された第1の情報処理装置で実行される、該第1の情報処理装置で読み取り可能且つ実行可能なプログラムを記録した記録媒体であって、該プログラムは、第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報とを、前記第2の情報処理装置に送信するステップと、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む。

【0042】更に、本発明に係るプログラムは、第1の記録媒体が装着される第1の情報処理装置とネットワークを介して接続される第2の情報処理装置で実行される、該第2の情報処理装置で読み取り可能且つ実行可能なプログラムであって、該プログラムは、第1の情報処理装置に関連した固有の情報と、第1の記録媒体に関連した固有の情報とを前記第1の情報処理装置から受信するステップと、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む。

【0043】更に、本発明に係るプログラムは、第1の記録媒体が装着される第1の情報処理装置であって、第2の情報処理装置とネットワークを介して接続された第1の情報処理装置で実行される、該第1の情報処理装置で読み取り可能且つ実行可能なプログラムであって、該プログラムは、第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報とを、前記第2の情報処理装置に送信するステップと、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む。

【0044】

【発明の実施の形態】以下、添付の図面を参照しながら本実施形態について詳細に説明する。

〔ディスク認証システム〕

（システム全体）図1は、本実施例に係るディスク認証システム全体の概念図である。図1に示されるように、ユーザ端末機器1が、ネットワーク3を介して認証用サーバ4と接続されている。この認証用サーバ4は、ネットワーク3を介して1又は2以上のコンテンツサーバ6と接続されている。これらのコンテンツサーバ6にはデバッグ専用サーバ6-4があってもよい。

【0045】ユーザ端末機器1は、アプリケーションプログラムを記録したCD-ROM（Compact Disc-Read

Only Memory）、DVD-ROM（Digital Versatile Disc-ROM）等の光ディスク2を搭載可能なコンピュータである。本実施例では、ゲーム機等に代表されるエンタテインメントシステムを例にとって説明する。このユーザ端末機器1はエンタテインメント本体装置に該当し、エンタテインメント本体装置に関しては、後で図2を用いてその内部の構成を説明する。なお、光ディスク2は、例示であって、これに限定されない。アプリケーションプログラム等のコンテンツを記録した種々の記録媒体全てが対象となることを承知されたい。例えば、外部接続のハードディスク（図示せず。）、後述のコネクタに接続されるメモリカード又はPDA内のメモリ等にアプリケーションプログラム等のコンテンツが記録されている場合には、これらは対象となる。しかし、説明を分かり易くするため、光ディスク2を例にとって説明する。

【0046】ネットワーク3としては、テレビジョンケーブルネットワーク、光ファイバネットワーク、xDSL（x Digital Subscriber Line）等のいわゆるブロードバンドネットワークが好ましい。また、既存の又はこれから構築される広帯域無線ネットワーク、携帯電話及びPHS（Personal Handyphone System）電話関連のネットワーク、インターネット関連のネットワーク等も利用することができる。

【0047】認証用サーバ4は、エンタテインメント装置1に接続され、エンタテインメント装置1及び記録媒体2が真正であるか不正であるかの認証を行うために用いられるサーバである。認証用サーバ4は、各々のエンタテインメント本体装置1に付与された固有のIDである機器ID（「SET ID」とも言う。）情報と、各々のユーザに付与された固有のIDであるユーザID（「USER ID」とも言う。）情報（パスワードを含む場合もある。）と、各々の光ディスク2に付与された固有のIDであるディスクID（「DISK ID」とも言う。）等のユーザ情報を蓄積するユーザデータベース5を有する。これらのIDは、各々単一のものであり、同じIDは2つ以上存在しない。特に、ディスクIDは、光ディスク1枚毎に付された相異なる識別記号である。

【0048】また、コンテンツサーバ6は、ユーザに提供し得る種々のデジタルコンテンツを蓄積したデータベース7を夫々有している。

【0049】更に、認証用サーバ4の代わりに、エンタテインメント装置1を用いることもできる。即ち、複数のエンタテインメント装置1が接続されて、その内の特定の一台が認証用サーバの役割を果たす場合である。この場合、これに接続されるユーザデータベース5は、ハードディスクのような記録媒体で構成される。

【0050】（装置本体の内部構成）図2は、図1のユーザ端末として利用されるエンタテインメントシステム

の本体装置の内部構成のブロック図である。図中、一点鎖線内はエンタテインメント本体装置 1 を、破線内は該エンタテインメント本体装置 1 のディスクドライブ 30 を、夫々示している。

【0051】エンタテインメント本体装置 1 は CPU 16 を有し、この CPU 16 はメインメモリ (RAM) 17 と接続されている。また、CPU 16 は描画装置 (GPU) 18 と接続されており、GPU 18 からの映像信号は、CRT-CTR (Cathode Ray Tube-Control)

(図示せず。) を介して表示装置 (CRT) (図示せず。) に出力されている。また、CPU 16 は、USB (Universal Serial Bus) コネクタ 14、IEEE1394 又は i リンク (i.LINK (登録商標)) コネクタ 15 等を有する IOP (Input/Output Processor) 13 を介して、コネクタ (コントローラ (PAD) / PDA (Personal Digital Assistant) / メモリカード・コネクタ) 12 に接続されている。

【0052】このコネクタ 12 には、メモリカード 11、コントローラ (PAD) 10、携帯端末 (PDA: Personal Digital Assistant) 等が接続される。このメモリカード 11、PDA 等は、外部記憶装置の一種であり、後述するように、ディスク ID、機器 ID 等が記録される。

【0053】また、CPU 16 は、IOP 13 を介してバス 27 に接続され、このバス 27 には、MASK-ROM (Masked ROM) 19、CD/DVD-DSP (CD/DVD-Digital Signal Processor) 22、DVD プレイヤ ROM 20、SPU (Sound Processing Unit) 25、ネットワーク・インターフェース 26 等が接続されている。SPU 25 からの音声信号は、アンプ、スピーカ等 (図示せず。) に出力されている。エンタテインメント本体装置 1 は、ネットワーク・インターフェース 26、USB コネクタ 14、i リンクコネクタ 15 等を介してネットワークと接続され、更にネットワークを通じて認証用サーバ 4、デジタルコンテンツサーバ 6 等に接続される。

【0054】CD/DVD-DSP 22 は、メカニカル制御部 23 及びドライブ 24 を介して、ディスクドライブ 30 の機械的制御を行う。この制御は、RF-AMP (Radio Frequency Amplifier) 21 を通じて行われる。また、CD/DVD-DSP 22 は、RF-AMP 21 を通じて、ディスクドライブ 30 の電氣的制御を行う。

【0055】光ディスク 2 は、スピンドルモータ (図示せず。) の機械的制御により回転される。また、光ディスク 2 に対しては、アクチュエータ (図示せず。) の電氣的制御によりピックアップレンズ (図示せず。) が駆動されて情報の記録/再生が行われる。

【0056】このエンタテインメント装置 1 は、製造番号等の固有の ID である機器 ID を有している。この機

器 ID は、例えば予めマスク ROM 19 に書き込まれるようにハードウェア的に組み込まれたもの、或いは後から光ディスク 2、メモリカード 11、携帯端末、コントローラ 10 等を介してソフトウェア的に読み込まれたものの、のいずれでもよい。

【0057】また、この光ディスク 2 にはディスク ID が記録されており、このディスク ID は後述する方法で読み取られる。

〔ディスク ID 認証システム〕

(第 1 のディスク ID 認証システム) 以下、図 3 を用いて第 1 のディスク ID 認証システムのエンタテインメント本体装置側の処理に関して具体的に説明し、図 4 を用いて認証用サーバ 4 側の処理に関して具体的に説明する。なお、本実施例においては、エンタテインメントシステムはゲーム機であり、ゲームプログラムを記憶した記録媒体としては CD-ROM のような光ディスクを使用し、更にディスク ID が通常のデータエリア以外のエリア (例えば、リードインエリアの内側、リードアウトの外側等) に存在する場合を前提として説明する。

【0058】図 3 は、エンタテインメント本体装置側の処理を示している。まず、エンタテインメント本体装置における処理の基本を説明する。ここで使用されている光ディスクは、通常では記録対象となっていないエリアにディスク ID が記録されている。このディスク ID の記録箇所を特定する情報 (例えば、アドレス) は、通常のデータエリアに記録されている。光ディスク 2 にディスク ID を記入するための材料としては、追記型ディスクに使用されている有機色素が一例として挙げられる。エンタテインメント本体装置は、ディスク情報を読み取り、そこからディスク ID の記録されたアドレスを検索し、更にこのアドレスに従ってディスク ID を読み取り、それを認証用サーバ 4 に送信している。以下、具体的に説明する。

【0059】ステップ S102 において、エンタテインメント本体装置 1 は、CPU の制御のもと、搭載された CD-ROM から TOC (Table of Contents) の基礎データを読み込む。そして、ステップ S103 において、CD-ROM のデータエリアのボリューム識別子 VD (Volume Description) を読み込み、ディスク ID の記入してあるアドレスを検索する。

【0060】ステップ S104 では、ボリューム識別子 VD にディスク ID のアドレスが存在するか否かが判定される。ID のアドレスが存在しなければ、搭載された CD-ROM は、このディスク ID 認証システムによる保護対象以外の CD-ROM と判定され、ステップ S113 に進行し、プログラムが実行される。このエンタテインメント本体装置 1 は、単にゲーム機として機能するだけでなく、音楽用 CD 再生装置、映画用 DVD 再生装置等としても機能する。このため、エンタテインメント本体装置に、ID 認証システムによる保護対象以外の光ディスク

(例えば、DVD-Video、Audio-CD、従来のゲームCD等)が搭載されている場合があり、このような場合はそのまま音楽や映像の再生やゲームの実行が行われる。

【0061】ボリューム識別子VDにIDアドレスが存在する場合、ステップS105において、ディスクIDを読み取るために、IDアドレスに従って光ディスクドライブ30のピックアップをCD-ROMのディスクIDデータ部(リードインエリア内側又はリードアウトの外側に設けられた部分)に向けてスライドさせる。このピックアップのスライド制御は、CPU16から出力されたスライド命令に基づいて、メカニカル制御部23にて行われる。

【0062】ステップS106において、CPU16は、CD-ROM上のディスクIDデータ部に、実際にディスクID情報が存在するか否かを判別する。ディスクID情報が存在しない場合又はディスクID情報の読み込みが不可能な場合には、ディスクID無しと判定され、ステップS107に進む。このステップS107では、プログラムの実行は拒否され、強制終了される。

【0063】ディスクIDデータ部に実際にディスクID情報が存在する場合、エンタテインメント本体装置1は、ステップS108において、CPUの制御の下、ディスクID情報を読み取りこれをメインメモリ17に記憶する。

【0064】ステップS109において、エンタテインメント本体装置1のCPU16は、ディスクIDのデータを、USB、IEEE(Institute of Electrical and Electronic Engineers)1394、PCMCIA(Personal Computer Memory Card International Association Architecture)等の規格に準拠した各種通信インターフェイスを介して、認証用サーバ4に対して送信する。そして、ステップS110で、送信したディスクIDに対して認証用サーバが認証処理を行うのを待つ。

【0065】ステップS111において、エンタテインメント本体装置1は、認証用サーバでの認証処理結果を受信する。認証用サーバでの認証処理の結果が「認証適」であれば、CD-ROMの読み取り許可命令が受信される。認証処理の結果が「認証否」であればステップS112に進み、プログラムの実行が拒否されて強制終了される。

【0066】認証用サーバでの認証処理の結果が「認証適」の場合、ステップS113において、エンタテインメント本体装置1のCPUは、CD-ROMに記録されたプログラムを実行する。

【0067】図4は、第1のディスクID認証システムにおける認証用サーバ4側の処理を示している。まず、認証用サーバ4における処理の基本を説明する。エンタテインメント本体装置1を購入したユーザは、その直後に、自分の氏名等のユーザIDと、各本体機器に付与さ

れた機器IDとを認証用サーバ4のユーザデータベース5に登録している。また、新たなゲームプログラムを購入したユーザは、その最初の使用時にディスクID情報を認証用サーバ4のユーザデータベース5に送信しなければ、そのプログラムの実行が出来ない(ステップS109参照)。このため、認証用サーバ4のユーザデータベース5には、ユーザ情報として、少なくともディスクIDと、更に、これと関連するユーザID、機器ID等の任意のものが蓄積される。ユーザ情報は、ユーザが複数の種類のゲームプログラムを購入すると、1つのユーザID及び機器IDに対して複数のディスクIDの組み合わせとなる。ユーザ情報は、テーブル化されてユーザデータベース5に蓄積される。

【0068】このような状況下で、ユーザがゲームを開始する場合、ユーザが使用しているディスクIDと機器IDの情報が、エンタテインメント本体機器1から認証用サーバ4に送信され、認証用サーバ4のユーザデータベースに蓄積されたユーザ情報と比較される。この比較結果は、図7に示すように、次の4通りとなる。

【0069】(No.1)ディスクIDと機器IDの両方が、蓄積されたものと一致する。

【0070】(No.2)ディスクIDのみが、蓄積されたものと一致する。

【0071】(No.3)機器IDのみが、蓄積されたものと一致する。

【0072】(No.4)ディスクIDと機器IDのいずれも、蓄積されたものとは一致しない。

【0073】No.1の、送信されたディスクIDと機器IDの組み合わせが、既にユーザデータベースに登録されたこれらに対応する情報と一致した場合、このディスクは正規のディスクと判断される。しかし、希なケースとして、機器IDが不正にコピーされ、且つディスクIDも不正にコピーされたような場合が起こる可能性がある。このようなケースを排除するため、同一のディスクIDと機器IDの組み合わせの認証要求が、同じ時間帯に重複した場合は不正使用であると判断し、この不正使用をカウントしてユーザデータベース5に記録すると共に、プログラムの実行を拒否する。

【0074】No.2の、送信されたディスクIDと機器IDの組み合わせの内、ディスクIDのみがデータベースに蓄積されたものと一致した場合、次の3通りの状況が考えられる。

【0075】(1)ディスク所有者が自分のディスクを他人に貸与した場合

(2)ディスク所有者が自分のディスクを他人の機器で実行した場合

(3)不正コピーの場合

これらのいずれに該当するかは、ディスクIDと共に登録されている機器IDのユーザに確認を求めることにより、判別できる。このエンタテインメントシステムは、



各エンタテインメント本体装置1が認証用サーバ4に対して接続されていることにより、このような確認作業が可能となる。

【0076】No. 3及びNo. 4の、送信されたディスクIDと機器IDの組み合わせの内、ディスクIDが未登録の場合、ディスク2の初回使用と判断され、ユーザデータベース5にディスクIDが登録される。以下具体的に説明する。

【0077】ステップS202において、認証用サーバ4は、ユーザが使用するエンタテインメント本体装置1に対する接続認証を行う。ここで、本体装置1の機器IDが、本体装置1からの送信データの一部として自動的にサーバに供給されるなら、ユーザはユーザIDであるパスワードのみを入力すればよい。接続認証に失敗した場合、ステップS203において、ユーザ端末装置と認証用サーバ4の間の接続は遮断される。接続認証が成功すれば、ステップS204において、ユーザの本体装置1との通信接続が確立される。

【0078】ステップS205において、認証用サーバ4は、エンタテインメント本体装置1からディスクIDデータ及び機器IDを受信する。これは図3のステップS109に対応する処理である。

【0079】ステップS206において、認証用サーバ4は、受信したディスクID、機器IDと、ユーザデータベース5に記録されているユーザ情報（ディスクID、機器ID）との比較を行う。

【0080】ステップS207において、受信したディスクIDが、データベース5に登録されたディスクIDと一致しているか否かが判定される。即ち、受信したディスクIDが、ユーザデータベース5上のテーブルになれば、そのディスクは初回の使用である。この場合はステップS208に進み、認証用サーバ4は、データベース5へのディスクIDの登録を行う。そして、ステップS212で、プログラム実行許可命令をエンタテインメント本体装置1に送信する。

【0081】送信ディスクIDがデータベース5に登録済みであれば、ステップS209に進み、受信機器IDと、前記ディスクIDの使用機器として登録された機器IDとが一致しているか否かが判断される。機器IDが不一致の場合、ステップS210に進み、ディスクIDに対応する機器IDのユーザ（ディスク所有者）に対して、使用許可の確認をする。ステップS211で、ディスク所有者が承諾すれば（即ち、ディスク所有者が、ディスク使用を許諾する旨をサーバ4に返信すれば）、これはディスク所有者が自分のディスクを他人に貸与したか、他のエンタテインメント本体装置1を利用して実行しているかであり、ステップS212で、プログラム実行許可命令をエンタテインメント本体装置1に送信する。

【0082】ディスク所有者が承諾しない場合、不正使用と判断され、ステップS214で不正使用のカウントがな

され、ステップS215で、プログラム実行拒否命令がエンタテインメント本体装置1に送信される。これにより、中古品等の不正使用が排除される。

【0083】ディスクIDと機器IDの組み合わせがユーザデータベース5に登録されているユーザ情報と一致していた場合でも、極めて希なケースであるが両方のIDが不正にコピーされた場合には、これを排除する必要がある。ステップS213で、同じ時間帯に同じディスクIDー機器IDの組み合わせでの使用が重複しているか否かが判断される。同時使用が発生していない場合、ステップS212で、プログラム実行許可命令がエンタテインメント本体装置1に送信される。同時使用が発生している場合、不正使用と判断され、ステップS214で不正使用のカウントがなされ、ステップS215で、プログラム実行拒否命令がエンタテインメント本体装置1に送信される。

【0084】通常、不正ディスクは真正なディスク内容をそのままコピーするため、データエリアに記録されたディスクIDのアドレスデータもコピーされてしまう。しかし、本実施の形態のフォーマットにおける、リードインエリアの内側又はリードアウトエリアの外側等のデータエリア以外に記録されたID情報は、真正ディスクをそのままコピーした不正ディスクにはコピーされない。これにより、不正ディスクにはディスクIDのアドレスに関する情報はコピーされているにもかかわらず、ディスクID自体が存在しないので、不正ディスクに対しては、図3のステップS104でディスクIDのアドレス有りと判定され、次いでステップS106でディスクID自体なしと判定されることにより、ステップS107でプログラムの実行が排除されることとなる。

【0085】ディスクIDの記録方法は、上述の方法に限定されない。例えば、ディスクIDは、データエリア内に、ビット列の物理的な変動を利用した方法で形成することも出来る。このビット列の物理的な変動を利用した方法は、ビット列の半径方向の変動（ウォブリング）、ビットサイズの短径方向の変動又はビットの深さ方向の変動のいずれかを利用することが出来る。或いは、ディスクIDは、電子透かし(Digital Watermark)を利用した方法で形成することも出来る。

【0086】認証用サーバへのディスクIDの登録方法は、上述の方法に限定されない。なお、特別な場合として、例えば光ディスク等の記録媒体の提供者自身が認証用サーバ4を提供するような場合がある。この場合には、自ら製造・提供するディスクIDは、予め認証用サーバ4のデータベース5に登録・蓄積しておくことが出来る。このような場合、第1のディスクID認証システムでは、初回使用時のディスクIDの登録処理は不要となる。

【0087】また、機器IDは必ずしも必要でない。機器IDは各々のユーザ固有のユーザIDで置き換えることが出来る。即ち、使用機器を特定する代わりに、ユー

ザを特定し、ユーザIDとディスクIDとの組み合わせにより、認証システムを機能させることが出来る。この場合、好ましくは、ユーザIDはパスワードの形式で付与される。

【0088】光ディスク等の記録媒体の提供者自身が認証用サーバ4を提供するような場合について、更に説明する。

【0089】この記録媒体提供者が、ディスク製造時に、ディスク一枚毎に個別の製造番号を与え、これをディスクIDとしてディスク2内に情報として組み込む。同時に、ユーザデータベース5には、そのディスクID（製造番号）が記録されている。一方で、エンタテインメント装置1の製造時に、エンタテインメント装置一台毎に個別の製造番号を与え、これをエンタテインメント装置内に機器IDとして組み込まれている。そして同時に、ユーザデータベース5には、その機器ID（製造番号）が記録されている。

【0090】この場合、ディスク2の工場出荷時には、ディスクIDは、エンタテインメント装置1の機器IDと未だ関連付けられていない。

【0091】ディスク2の利用者が、認証用サーバ4に対して接続・認証処理の要求を行う（S109）と、認証用サーバ4は機器ID認証後に、ディスクIDの認証を行う。

【0092】ユーザデータベース5には、予め機器ID、ディスクID（ユーザ情報）が記録されているので、認証用サーバ4はエンタテインメント装置1から受信した機器ID-ディスクIDがこのユーザデータベース5に記録されたユーザ情報に該当するか否かをチェックする。

【0093】その結果、ユーザデータベース5のユーザ情報に該当するものがなかった場合には、認証を強制終了してディスク2のプログラム実行を拒否する。この際、不正なディスクIDをユーザデータベース5に蓄積するようにしておけば、各エンタテインメント装置毎の不正なディスクを利用した認証用サーバ4へのアクセス回数のカウントや、不正ディスクを利用したエンタテインメント装置1の特定等の不正ディスクに関わる管理が可能となる。

【0094】また、不正なディスクの排除以外に関しても、ディスクIDが付与されたディスク2を用いたアクセス回数のカウントは、本発明のネットワークシステムにおいて有効に利用することが可能である。即ち、認証用サーバ4へのアクセス回数を利用して、アクセス回数がある回数以上に達した時、認証を強制終了してディスク2のプログラム実行を拒否するようにすることも出来る。

【0095】例えば、IDが付与されたディスク2を用いた認証用サーバ4へのアクセス回数を管理することで、ディスク2に含まれるプログラム等のコンテンツに

対しお試し期間を設けてユーザに利用させることが可能である。これにより、ユーザはあるディスク2の利用回数がある一定回数に達するまでは、お試し期間としてディスク内のプログラム等のコンテンツを利用してゲームやサービス等を利用することが可能である。

【0096】現在、多くのインターネット接続サービス体験版ソフトは、利用時間をカウントすることでお試し期間を設けているが、本発明のネットワークシステムを用いれば、サービスの利用時間による管理ではなく利用回数による管理が可能となる。

【0097】例えば、音楽や映像を、本発明の認証用サーバ4を介してコンテンツサーバ6からエンタテインメント装置1に対してダウンロード提供するサービスに利用可能である。ここで、サービスに加入したユーザは、サービス提供者からサービス利用のためのディスク2を配布されるものとする。ディスク内には、ディスク毎に付与されたディスクIDと共に、認証用プログラム、ダウンロード実行用プログラム等が記録されている。ユーザは、このディスク2をエンタテインメント装置1に装着することで認証用サーバ4並びにコンテンツサーバ6に接続することが可能となり、これにより音楽や映像等をダウンロード可能となる。

【0098】この際、ダウンロード回数をディスクIDを付与したディスク2を用いたコンテンツサーバ6へのアクセス回数として認証用サーバ4がカウントすれば、ダウンロード（通信）時間に依存しない、サービスの利用回数制限が実現可能となる。

【0099】更に、認証用サーバ4においてユーザがアクセスしたコンテンツ内容を表す情報とユーザ情報（機器ID、ユーザID、ディスクID等）とを相互に関連付けてユーザデータベース5内に蓄積していけば、ユーザ毎の嗜好等を容易に管理することが可能となる。これらの蓄積情報を用いて、サービス提供者或いはコンテンツ提供者は各ユーザ毎に適切な広告等をインターネット等の通信回線を通じて提供することが可能となる。

【0100】以上は利用回数に応じた、サービス提供等の利用制限方法であったが、制限方法はこれに限られない。例えば、ディスクIDが付与されたディスク2に記録された内容を、サービス提供者がユーザからの徴金状況に応じて、制限を付けて提供することもできる。ディスク2に記録された内容は、すべてを利用可能ではなく部分的に利用可能であるとする。ユーザが、その部分的に利用できない内容を利用したい時には、ユーザはその利用内容に応じた対価をサービス提供者に支払うこととなる。サービス提供者は、それを受けて、ユーザによる利用を可能とする。

【0101】例えば、ディスク2に記録された内容を部分的に暗号化しておけば、利用対価を支払わないユーザは暗号部分に相当する利用できないが、利用対価を支払ったユーザに対しては、暗号を解読するための鍵をサー

ビス提供者からユーザのエンタテインメント装置1に提供を行うことで、利用可能となる。前記サービス提供者からエンタテインメント装置1に対して送信される情報は、暗号解読用の鍵には限られない。

【0102】また、ユーザがディスク2の部分的に利用できない記録内容を利用するためにサービス提供者に対して行うのは、対価の支払いに限られず、例えばユーザのエンタテインメント装置1からサービス提供者が運営する認証用サーバ4への、ユーザIDの送信であってもよい。このユーザIDは、サービス提供者から各ユーザに対して予め付与されたIDであってもよい。

【0103】（第2のディスクID認証システム）次に、第2のディスクID認証システムについて説明する。第2のディスクID認証システムでは、認証対象となるディスクは、CD-ROM等に限定されず、TOCの規定されていないDVD-ROM等も含められる。また、ディスク内のディスクIDの記録箇所も限定されず、リードインエリアの内側、リードアウトの外側、又はデータエリア内のいずれの箇所であってもよい。

【0104】上記第1のディスク認証システムと比較すると、第1のディスク認証システムでは、ゲームをプレイするためにディスク上のプログラムを起動する毎に、サーバに接続して認証を行っていたが、この第2のディスク認証システムでは、ユーザ情報をメモリカード11等の本体接続型の外部記憶装置に記憶することで、サーバに接続する処理行程を省略している。即ち、ディスクの初回使用時に、メモリカード11等にディスクID-機器IDのユーザ情報を記録し、ゲーム実行毎にこのユーザ情報を利用してディスクの認証を行っている。なお、外部記憶装置には、アプリケーションプログラム等のコンテンツが記録されていてもよい。

【0105】図5を用いて第2のディスクID認証システムのエンタテインメント本体装置側の処理について具体的に説明し、図6を用いて認証用サーバ4側の各ステップでの処理内容について具体的に説明する。

【0106】ステップS302で、エンタテインメント本体装置1は、CPU16の制御の下、装着ディスク2に記録されている固有の基礎データをメインメモリ17に読み込む。装着ディスク2は、CD、CD-ROM、DVD-Video、DVD-ROM等の各種ディスクが含まれる。

【0107】ステップS303では、読み込んだ基礎データの中にディスクIDが有るか否かが判断される。ディスクIDが存在しなければ、認証対象以外のディスクであると判断され、ステップS312に進み、プログラムが実行される。

【0108】ディスクIDが存在する場合、ステップS304に進み、CPU16の制御の下、エンタテインメント本体装置に接続されたメモリカード11等の外部記憶装置に記録されたユーザ情報（ディスクID-機器IDの

組み合わせデータ）が読み込まれる。なお、このメモリカード11等には、ゲームのハイスコア、前回中断したゲームの進行状況のバックアップデータ等のデータも記録されている。

【0109】ステップS305では、メモリカード11にディスクIDが記録されているか否かが判断される。ディスクを最初に使用した時に、メモリカード11のユーザ情報にディスクIDと機器IDとが登録されるため、2回目以降の使用時には、メモリカード11に、ディスクIDがユーザ情報として記録されていることになる。従って、メモリカード11にディスクIDの記録が無い場合としては、①ディスクの初回使用時、②メモリカード自体の交換時、等が考えられる。読み取ったディスクIDがメモリカード等に記録されていた場合、ステップS306に進む。

【0110】ステップS306では、メモリカード11等に記録されているディスクIDが、装着ディスクのディスクIDと一致するか否かが判断される。一致しない場合としては、ディスクの初回使用時その他が考えられる。一致していれば、ステップS307に進む。

【0111】ステップS307において、メモリカード11から読み込んだ機器IDが、現在使用している本体装置の機器IDと一致するか否かが判断される。一致しない場合としては、ディスク所有者からディスク2とメモリカード11とを借りてきたユーザが、自らの本体装置でゲームをする場合等が考えられる。一致する場合（ディスクID-機器IDの組み合わせが、ディスク購入時にメモリカード等に記録したユーザ情報と一致している場合）、正当使用に該当し、ユーザ認証を完了して、ステップS312でプログラムが実行される。

【0112】ステップS305で、メモリカードにディスクIDが存在しなかった場合、ステップS306で、メモリカード11等に記録されているディスクIDがディスクから読み込んだディスクIDと一致しなかった場合、又はステップS307で、メモリカード11等に記録されている機器IDが使用機器の機器IDと一致しなかった場合は、ステップS308に進む。このステップS308で、エンタテインメント本体装置は、USB、IEEE1394、PCMCIA等の通信インターフェイスを介して、ディスクID、使用機器の機器IDデータを認証用サーバ4に対して送信し、ステップS309でユーザ認証を待つ。この後、認証用サーバ4から、これらのディスクID、機器IDデータをメモリカード11に記録する命令を受信したときは、これらの書き込みを行う（図6のステップS405に対応）。

【0113】ステップS310で、認証用サーバ4での認証処理結果を元にプログラムの実行の可否を決定する。

「認証否」の場合、ステップS311に進み、プログラムの実行が拒否され、強制終了される。「認証適」の場合、ステップS312に進み、プログラムを実行する。

【0114】図6は、第2のディスクID認証システムにおける認証用サーバ4側の処理内容を示している。

【0115】ステップS402で、認証用サーバ4は、エンタテインメント本体装置に対する接続を確立した後、ディスクID、本体装置の機器IDを受信する。ディスクIDは、図5のステップS302でディスクから読み取られ、ステップS308で送信されたディスクIDであり、機器IDもステップS308で送信されたものである。

【0116】ステップS403で、受信したディスクIDが認証用サーバ4のユーザデータベースに蓄積されているディスクIDの中に存在するか否かが判定される。存在しない場合、そのディスクは初回使用と判断される。従って、ステップS404で、受信したディスクID－機器IDの組み合わせが、ユーザデータベース5にユーザ情報としてテーブル化して蓄積（登録）される。次いで、ステップS405で、ディスクID－機器IDを互に関連付けてユーザの本体装置1に接続されているメモリカード11等に記録させることで、図5で説明した認証処理を可能とする。

【0117】ステップS406で、認証用サーバ4は、使用ディスクに対するパスワードを本体装置1に送信する。このパスワードは、ディスクの所有者しか知り得ない秘密キーであり、後述するように、ユーザの意思確認のために使用される。このパスワードは、ユーザが使用する本体装置1の画面に対して出力されることが好ましい。ユーザはこのパスワードを書き留めておくことにより、他人へディスクを貸出すときにパスワードを教え、その他人がディスクを使用できるようにすることが可能となる。その後、ステップS414で、エンタテインメント本体装置に対してプログラム実行許可命令を送信する。

【0118】ステップS403で、受信ディスクIDが、登録されているディスクIDと一致した場合、ステップS407で、受信した機器IDが、前記ディスクIDに対応するデータベース中の機器IDと一致するか否かが比較され、ステップS408で、両者が一致するか否かが判定される。一度でも使用されたディスクに関しては、ユーザデータベース5にディスクID－機器IDの組み合わせからなるデータが蓄積されているため、このステップS408においては、機器IDがディスクIDに対応するものであるか否かを判別する。これにより、中古使用を排除することが出来る。メモリカード11の交換、メモリカードのディスクID－機器IDの記録の消失等の場合、ステップS409で、認証用サーバ4は、ディスクID－機器IDの組み合わせデータをエンタテインメント本体装置に送信してメモリカードに記録させる。その後、ステップS414で、エンタテインメント本体装置に対してプログラム実行許可命令を送信する。

【0119】ユーザデータベース5にディスクIDは存在するが、対応機器IDがデータベース中のものと一致しない場合、ステップS408からステップS410に進み、パ

スワードの入力要求をエンタテインメント本体装置1に送信する。この入力要求は、本体装置1に接続されたテレビジョンモニタ（図示せず。）に表示される。ステップS411で、ユーザから受信したパスワードが、正当か否かが判断される。正当であれば、ステップS412に進み、このディスクの借用者等に新たなパスワードを発行して送信する。ディスク借用者等がディスク所有者からディスクを合意のもとで借りるとき、このパスワードを入力することで、プログラム実行拒否命令を回避することが可能となる。この結果、ディスク借用者は、必ずしもディスク所有者から、ディスク2と共にメモリカード11を借りる必要が無くなる。また、ステップS412では、ディスク所有者に対して発行したディスク固有のパスワードを更新する。更新したパスワードはディスク所有者に対して送信される。これにより中古品の蔓延を助長することが回避できる。

【0120】ステップS412の後、ステップS414で、認証用サーバ4は、エンタテインメント本体装置に対してプログラム実行許可命令を送信する。

【0121】ステップS411で、ユーザから受信したパスワードが正当ではないと判断された場合は、ステップS413に進み、認証用サーバ4からエンタテインメント本体装置に対して、プログラム実行拒否命令が送信される。

【0122】上述した第1のディスクID認証システム及び第2のディスクID認証システムの実施例では、ユーザは、自分のエンタテインメント装置1に対して、手許にある光ディスクのような記録媒体からプログラムを読み込んでいる。しかし、本発明はこれに限定されない。例えば、ディスクIDが付与された記録媒体が他所にあり、遠隔操作により第1又は第2のディスクID認証システムを実行して認証許可を得た後で、その記録媒体に記録されたプログラムをダウンロードすることも出来る。或いは、例えば、ディスクIDが付与された記録媒体が他所にあり、その記録媒体に記録されたプログラムをダウンロードした後で、第1又は第2のディスクID認証システムを実行して認証許可を得て、プログラムを実行することも出来る。

【0123】

【発明の効果】本発明によれば、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムを有するコンピュータシステムを提供することができる。

【0124】更に、本発明によれば、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムを有するコンピュータシステムの使用方法を提供することができる。

【図面の簡単な説明】

【図1】図1は、ディスクID認証システムを説明する図である。

【図2】図2は、図1のエンタテインメント本体装置の

構成を示す図である。

【図3】図3は、第1のディスクID認証方法における本体装置側の処理のフローである。

【図4】図4は、第1のディスクID認証方法における認証用サーバ側の処理のフローである。

【図5】図5は、第2のディスクID認証方法における本体装置側の処理のフローである。

【図6】図6は、第2のディスクID認証方法における認証用サーバ側の処理のフローである。

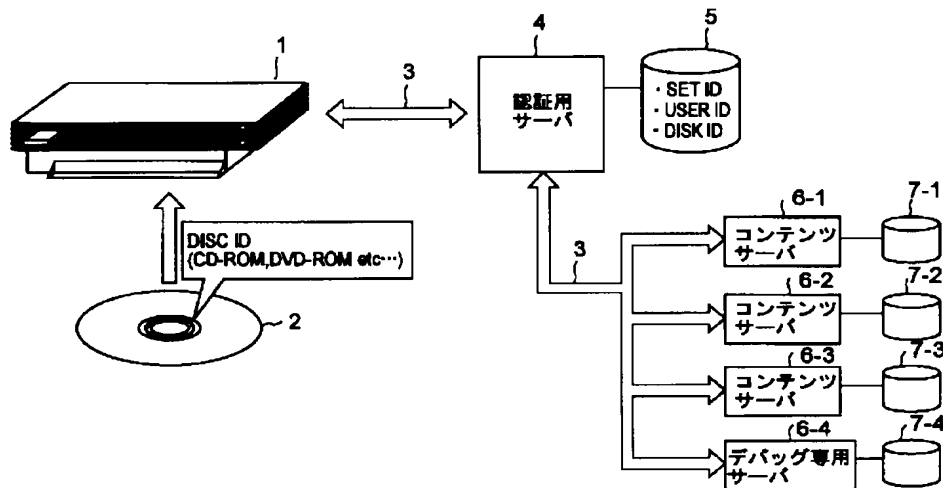
【図7】図7は、認証用サーバが受信したディスクID

及び機器IDと、ユーザデータベースに予め蓄積されたユーザ情報との比較結果を表す表である。

【符号の説明】

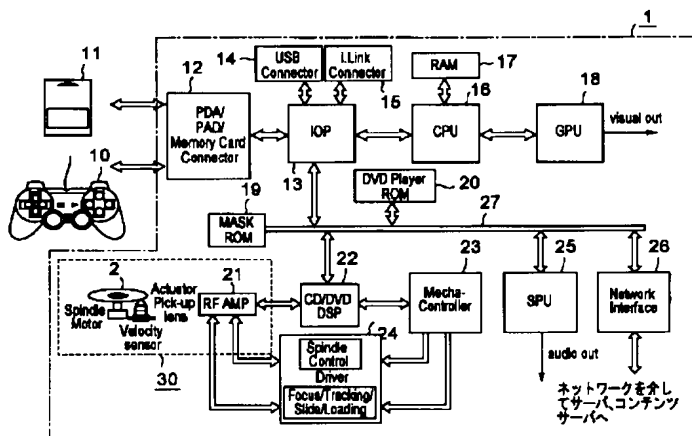
- 1：エンタテインメント本体装置（コンピュータ）
- 2：光ディスク（第1の記録媒体）
- 4：認証用サーバ
- 5：ユーザデータベース
- 6：コンテンツサーバ
- 7：データベース
- 11：メモ리카ード（第2の記録媒体）

【図1】



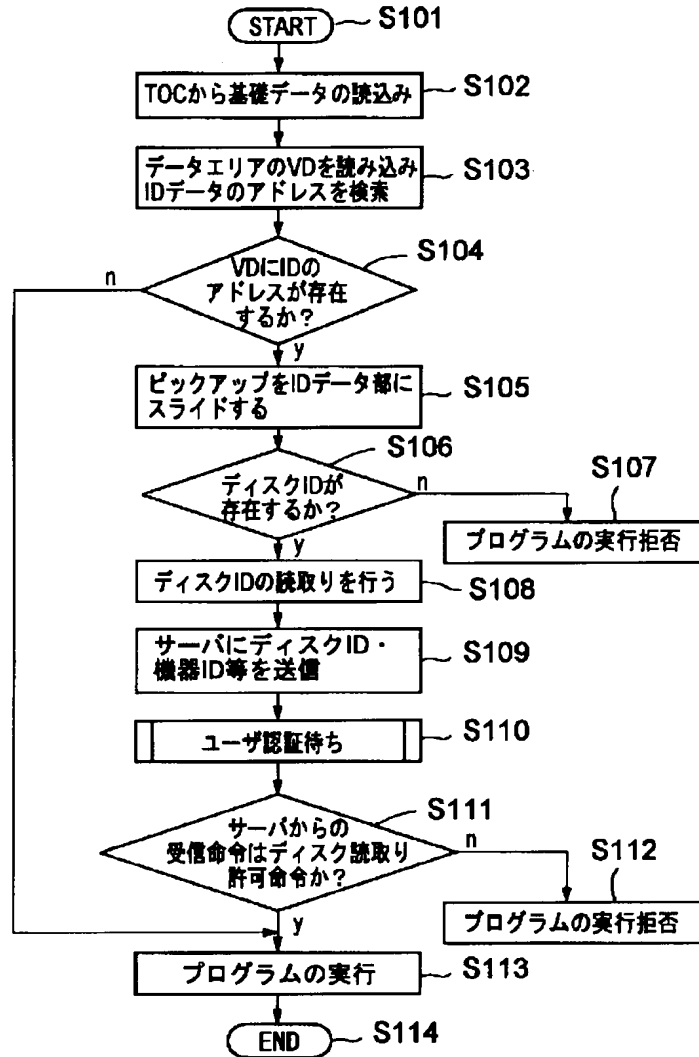
システムの概念図

【図2】



エンタテインメント本体装置の構成

【図 3】

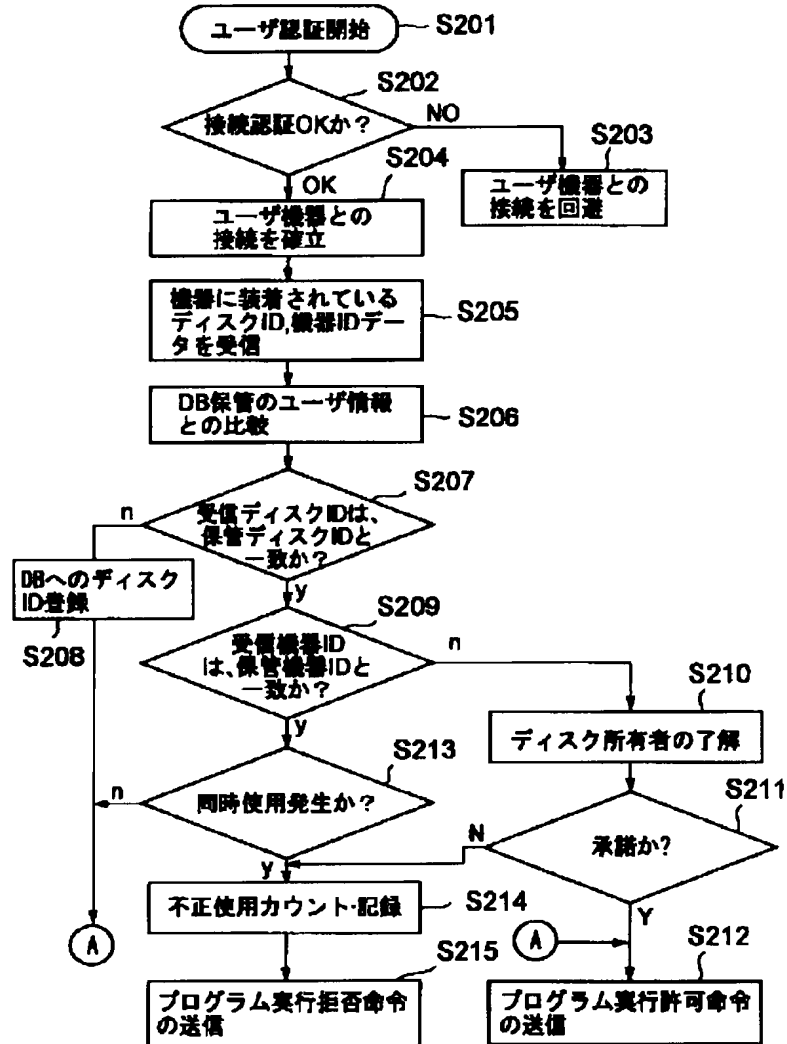


ディスクID認証（本体装置側処理）

【図 7】

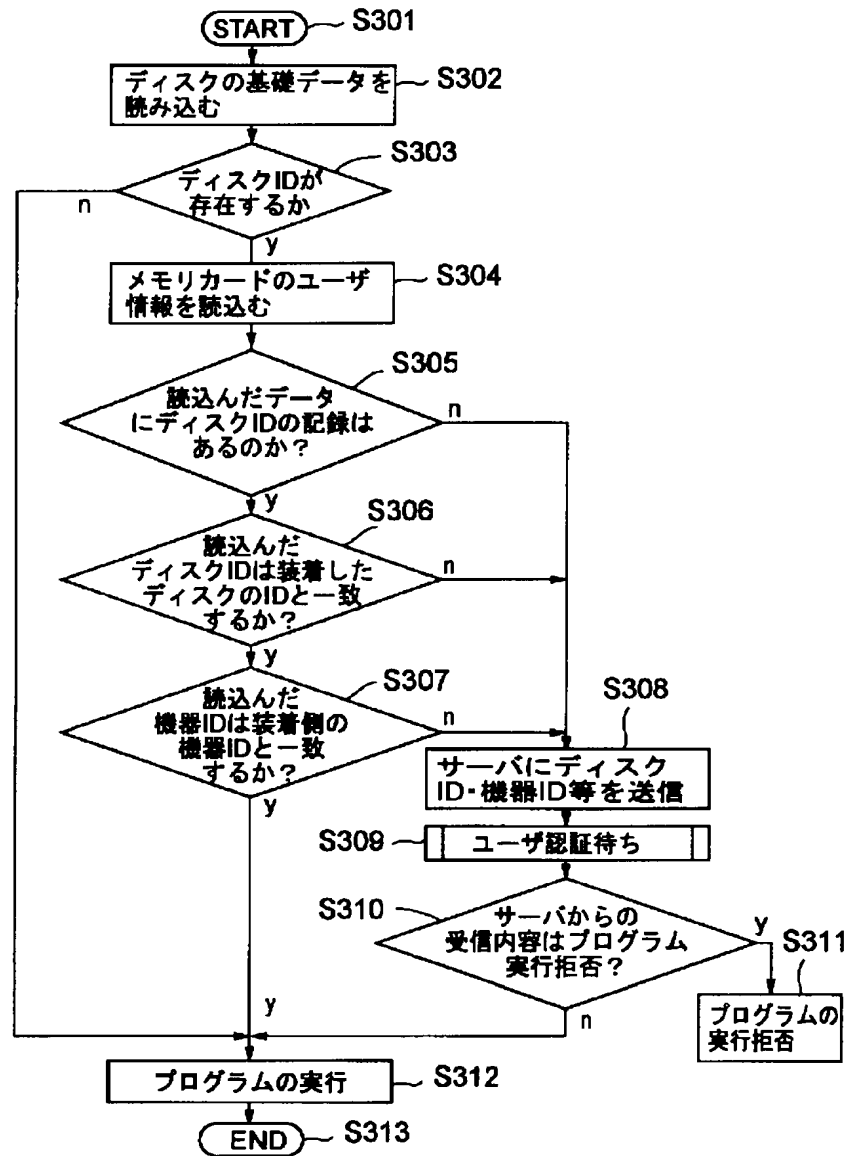
No.	送信情報	蓄積されたディスクID	蓄積された機器ID
1	送信ディスクID, 送信機器ID	○	○
2		○	×
3		×	○
4		×	×

【図4】



ディスクID認証(認証用サーバー側処理)

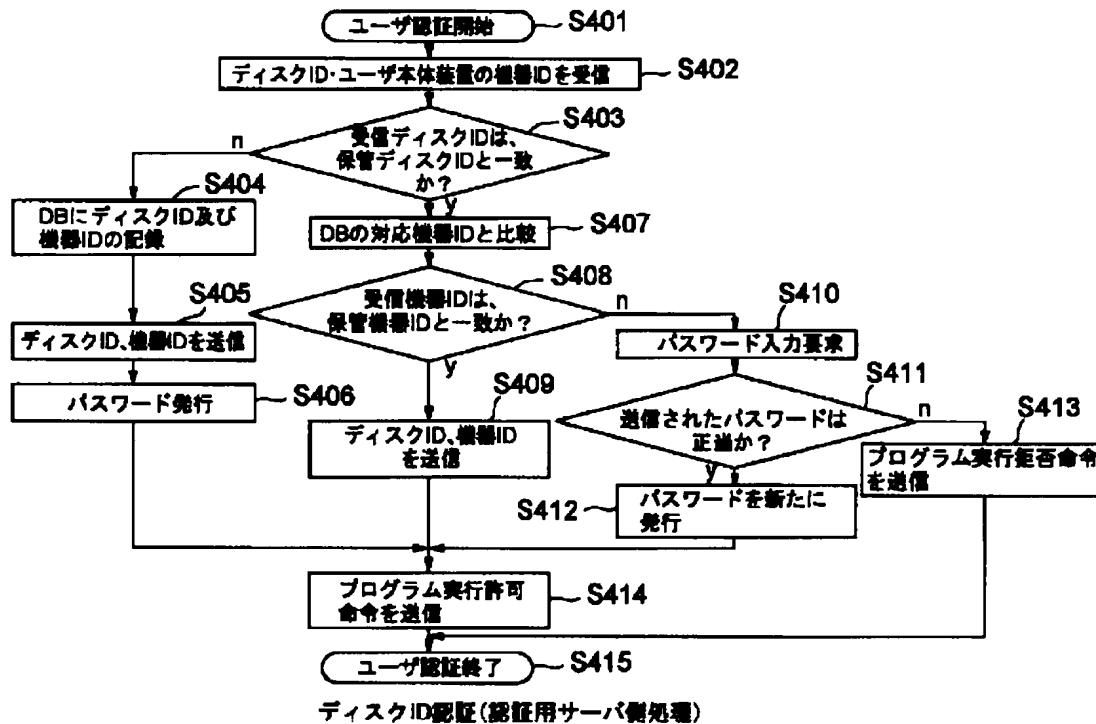
【図5】



ディスクID認証(本体側処理)



【図6】



フロントページの続き

(51) Int. Cl. 7  
G 1 1 B 27/00

識別記号

F I  
G 1 1 B 27/00

テーマコード(参考)

A

(72)発明者 岡本 伸一  
東京都港区赤坂7丁目1番1号 株式会社  
ソニー・コンピュータエンタテインメント  
内  
(72)発明者 三浦 和夫  
東京都港区赤坂7丁目1番1号 株式会社  
ソニー・コンピュータエンタテインメント  
内

Fターム(参考) 5B017 AA06 BB09 BB10 CA09 CA16  
5B065 BA03 PA00 PA11  
5D044 AB02 BC03 CC06 DE48 DE50  
DE54 FG18 GK12 HH15 HL02  
HL11  
5D090 AA01 BB02 CC04 FF24 GG17  
GG36  
5D110 AA15 BB01 BB24 DA04 DA12  
DB03 DC05 DE01 EA07